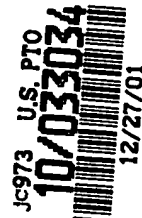


日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

2000年12月28日

出願番号
Application Number:

特願2000-403472

出願人
Applicant(s):

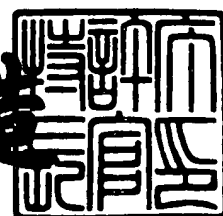
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 4月 6日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3025990

【書類名】 特許願

【整理番号】 0001076230

【提出日】 平成12年12月28日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 H04L 9/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 神谷 成樹

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 山下 雅美

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100067736

【弁理士】

【氏名又は名称】 小池 晃

【選任した代理人】

【識別番号】 100086335

【弁理士】

【氏名又は名称】 田村 榮一

【選任した代理人】

【識別番号】 100096677

【弁理士】

【氏名又は名称】 伊賀 誠司

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 配信方法及び配信システム

【特許請求の範囲】

【請求項 1】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の複数の鍵情報を生成する処理と、生成された複数の鍵情報をデジタルコンテンツとは別の配信経路（媒体を物理的に異にするもの、又は、配信時間帯を異にするもの。以下同じ。）であって、鍵情報相互間においても別の配信経路となるものを用いて配信する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、複数の配信経路を通じて配信を受けた複数の鍵情報を基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタ

ルコンテンツの元データをスクランブル処理して出力する処理とを実行させ、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項 2】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と記録媒体の形態で配信を受けた残りの部分とを基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされるこ

とを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項 3】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第 1 の伝送網を通じて各特定者に配信する処理と、生成された部分鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、上記部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を第 2 の伝送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第1の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第2の記録媒体の形態で配信を受けた部分鍵又はその発生情報と、伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理の解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項4】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテ

ンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第1の記録媒体に書き込む処理と、上記部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第2の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、伝送網を通じて配信を受けた部分鍵又はその発生情報と、第1の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第2の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報を基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項 5】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を第 1 の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を第 2 の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第 1 の伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と、第 2 の伝送網を通じて配信を受けたそれらと対をなす残りの部分とを基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理において生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理と

を実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項 6】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を記録媒体の形態での配信用に鍵専用の第 1 の記録媒体に書き込む処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の第 2 の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第 1 の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報の一部と、第 2 の記録媒体の形態で配信を受けたそれらと対をなす残りの部分とを基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツ

に付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項 7】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第 1 の伝送網を通じて各特定者に配信する処理と、残る部分鍵又はその発生情報を第 2 の伝送網を通じて各特定者に配信する処理と、上記部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を第 3 の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第1の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第2の伝送網を通じて配信を受けた残りの部分鍵又はその発生情報と、第3の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項8】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテ

ンツを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第1の記録媒体に書き込む処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第2の記録媒体に書き込む処理と、上記部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第3の記録媒体に記録する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第1の記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第2の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第3の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報を基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項 9】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の第 1 の暗号鍵を発生する処理と、デジタルコンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、上記第 2 の暗号鍵によって上記第 1 の暗号鍵又はその発生情報を暗号化し、伝送網を通じて特定者に配信する処理と、上記第 2 の暗号鍵を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、記録媒体の形態で配信を受けた第 2 の暗号鍵又はその発生情報を基に、伝送網を通じて配信を受けた第 1 の暗号鍵又はその発生情報に施されている暗号処理を解除して、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して

出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項 10】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の第 1 の暗号鍵を発生する処理と、デジタルコンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、上記第 2 の暗号鍵によって上記第 1 の暗号鍵又はその発生情報を暗号化し、第 1 の伝送網を通じて特定者に配信する処理と、上記第 2 の暗号鍵を基に配信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第 2 の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第 2 の伝送網を通じて配信を受けた合わせ鍵の一部と、記録媒体を通じて配信を受けた合わせ鍵の残

りの部分とから第2の暗号鍵を復元して、第1の伝送網を通じて配信を受けた第1の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項11】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の第1の暗号鍵を発生する処理と、デジタルコンテンツを第1の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第2の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、第2の暗号鍵によって暗号化された上記第1の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第1の記録媒体に書き込む処理と、上記第2の

暗号鍵を基に配信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第2の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、伝送網を通じて配信を受けた合わせ鍵の一部と、第2の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第2の暗号鍵を復元して、第1の記録媒体を通じて配信を受けた第1の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先であって、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項12】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システム

と、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の第1の暗号鍵を発生する処理と、デジタルコンテンツを第1の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第2の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、上記第2の暗号鍵によって上記第1の暗号鍵又はその発生情報を暗号化し、第1の伝送網を通じて特定者に配信する処理と、上記第2の暗号鍵を第2の伝送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第2の伝送網を通じて配信を受けた第2の暗号鍵又はその発生情報を基に、第1の伝送網を通じて配信を受けた第1の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サ

サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項 1 3】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の第 1 の暗号鍵を発生する処理と、デジタルコンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、上記第 2 の暗号鍵によって上記第 1 の暗号鍵又はその発生情報を暗号化し、記録媒体の形態での配信用に鍵専用の第 1 の記録媒体に書き込む処理と、上記第 2 の暗号鍵を記録媒体の形態での配信用に鍵専用の第 2 の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第 2 の記録媒体の形態で配信を受けた第 2 の暗号鍵又はその発生情報を基に、第 1 の記録媒体の形態で配信を受けた第 1 の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除された

ディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する処理と、復元されたディジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルコンテンツの唯一の出力先において、当該ディジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするディジタルコンテンツの配信方法。

【請求項 1 4】 特定者のみが視聴又は記録できるように暗号処理の施されたディジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたディジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルコンテンツの配信方法であって、

ディジタルコンテンツを供給する制作者システムと、供給を受けたディジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各ディジタルコンテンツに固有の第 1 の暗号鍵を発生する処理と、ディジタルコンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、ディジタルコンテンツに固有のものを発生する処理と、上記第 2 の暗号鍵によって上記第 1 の暗号鍵又はその発生情報を暗号化し、第 1 の伝送網を通じて特定者に配信する処理と、上記第 2 の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第 2 の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を第 3 の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルコンテンツを配信する処理とを実行し、

配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サ

サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第2の伝送網を通じて配信を受けた合わせ鍵の一部と、第3の伝送網を通じて配信を受けた合わせ鍵の残りの部分とから第2の暗号鍵を復元して、第1の伝送網を通じて配信を受けた第1の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項15】 特定者のみが視聴又は記録できるように暗号処理の施されたデジタルコンテンツを放送形式又は記録媒体の形態で配信する上流側システムと、配信を受けたデジタルコンテンツに施されている暗号処理を解除する下流側システムとの間で実行されるデジタルコンテンツの配信方法であって、

デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとを備える上流側システムがその制御下において、

各デジタルコンテンツに固有の第1の暗号鍵を発生する処理と、デジタル

コンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、第 2 の暗号鍵によって暗号化された上記第 1 の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第 1 の記録媒体に書き込む処理と、上記第 2 の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第 2 の記録媒体に書き込む処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第 3 の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行し、

配信を受けたデジタルコンテンツに施されている暗号処理を解除する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおいて、

正規の手続きによってのみ開封可能な上記復号サーバが、第 2 の記録媒体を通じて配信を受けた合わせ鍵の一部と、第 3 の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第 2 の暗号鍵を復元して、第 1 の記録媒体を通じて配信を受けた第 1 の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でス

クランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とするデジタルコンテンツの配信方法。

【請求項 1 6】 特定者のみが再生できるように暗号処理の施されたデジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムであって、

上記復号サーバは、配信段階でデジタルコンテンツに施された暗号処理を解除する暗号解除部と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、上記暗号解除部で暗号処理が解除されたデジタルコンテンツの唯一の出力先であって、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する復号化部と、復元されたデジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理部とを備え、

上記出力装置は、上記受信サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記受信サーバから与えられたスクランブル解除鍵によって解除するスクランブル解除部と、上記スクランブル解除部でスクランブルが解除されたデジタルコンテンツの唯一の出力先であって、当該デジタルコンテンツを所定の出力形態で再生する信号処理部とを備える

ことを特徴とする電子配信システムにおける下流側システム。

【請求項 1 7】 特定者のみが再生できるように暗号処理の施されたデジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバであって、

配信段階でデジタルコンテンツに施された暗号処理を解除する暗号解除部と

デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、

上記暗号解除部で暗号処理が解除されたデジタルコンテンツの唯一の出力先であって、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する復号化部と、

復元されたデジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理部とを備える

ことを特徴とする復号サーバ。

【請求項 1 8】 特定者のみが再生できるように暗号処理の施されたデジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバとしての回路装置であって、

配信段階でデジタルコンテンツに施された暗号処理を解除する暗号解除部と、

デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、

上記暗号解除部で暗号処理が解除されたデジタルコンテンツの唯一の出力先であって、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する復号化部と、

復元されたデジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理部とを備える

ことを特徴とする回路装置。

【請求項 1 9】 コンピュータを、特定者のみが再生できるように暗号処理の施されたデジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバとして、

配信段階でデジタルコンテンツに施された暗号処理を解除する暗号解除処理と、

デジタルコンテンツに付属する再生条件が満たされることを条件にスクラン

ブル鍵とその解除鍵とを局所的に生成するスクランブル制御処理と、

上記暗号解除部で暗号処理が解除されたデジタルコンテンツの唯一の出力先であって、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する復号化処理と、

復元されたデジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理と

を実行させるためのプログラムを記録した記録媒体。

【請求項 2 0】 特定者のみが再生できるように暗号処理の施されたデジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバであって、

配信段階でデジタルコンテンツに施された暗号処理を解除する暗号解除部と

上記暗号解除部で暗号処理が解除されたデジタルコンテンツの唯一の出力先であって、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する復号化部と、

復元されたデジタルコンテンツの唯一の出力先であって、スクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理部とを備える

ことを特徴とする復号サーバ。

【請求項 2 1】 特定者のみが再生できるように暗号処理の施されたデジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバとしての回路装置であって、

配信段階でデジタルコンテンツに施された暗号処理を解除する暗号解除部と

上記暗号解除部で暗号処理が解除されたデジタルコンテンツの唯一の出力先であって、当該デジタルコンテンツに施されている符号化処理を復号化し、デ

ィジタルコンテンツの元データを復元する復号化部と、

復元されたディジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理部とを備える

ことを特徴とする回路装置。

【請求項 2 2】 コンピュータを、特定者のみが再生できるように暗号処理の施されたディジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる復号サーバとして、

配信段階でディジタルコンテンツに施された暗号処理を解除する暗号解除処理と、

上記暗号解除部で暗号処理が解除されたディジタルコンテンツの唯一の出力先であって、当該ディジタルコンテンツに施されている符号化処理を復号化し、ディジタルコンテンツの元データを復元する復号化処理と、

復元されたディジタルコンテンツの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルコンテンツの元データをスクランブル処理して出力するスクランブル処理と

を実行させるためのプログラムが記録された記録媒体。

【請求項 2 3】 配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバであって、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部を備える

ことを特徴とする復号サーバ。

【請求項 2 4】 配信を受けたディジタルコンテンツに施されている暗号処理を解除する復号サーバとしての回路装置であって、ディジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部を備える

ことを特徴とする回路装置。

【請求項 2 5】 コンピュータを、配信を受けたディジタルコンテンツに施さ

れている暗号処理を解除する復号サーバとして、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御処理を実行させるプログラムを記録する記録媒体。

【請求項 2 6】 特定者のみが再生できるように暗号処理の施されたデジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる出力装置であって、

上記受信サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記受信サーバから与えられたスクランブル解除鍵によって解除するスクランブル解除部と、

上記スクランブル解除部でスクランブルが解除されたデジタルコンテンツの唯一の出力先であって、当該デジタルコンテンツを所定の出力形態で再生する信号処理部とを備える

ことを特徴とする出力装置。

【請求項 2 7】 特定者のみが再生できるように暗号処理の施されたデジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる出力装置としての回路装置であって、

上記受信サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記受信サーバから与えられたスクランブル解除鍵によって解除するスクランブル解除部を備える

ことを特徴とする回路装置。

【請求項 2 8】 コンピュータを、特定者のみが再生できるように暗号処理の施されたデジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムに用いられる出力装置として、

上記受信サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記受信サーバから与えられたスクランブル解除鍵によって解除するスクランブル解除処理

を実行させるプログラムを記録した記録媒体。

【請求項 2 9】 特定者のみが再生できるように暗号処理の施されたデジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを再生する出力装置とを備える下流側システムにおける信号処理方法であって、

正規の手続きによってのみ開封可能な上記復号サーバが、配信段階でデジタルコンテンツに施された暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、上記処理で暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行する

ことを特徴とする下流側システムにおける信号処理方法。

【請求項 3 0】 特定者のみが再生できるように暗号処理の施されたデジタルコンテンツの配信を受けて所定の信号処理を実行する復号サーバにおける信号処理方法であって、

正規の手続きによってのみ開封可能な上記復号サーバが、配信段階でデジタルコンテンツに施された暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツの元データを復元する処理と、復元されたデジタルコン

テンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツの元データをスクランブル処理して出力する処理とを実行する

ことを特徴とする復号サーバにおける信号処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はデジタルコンテンツの配信方法及び配信システムに関する。また、本発明は、デジタルコンテンツの配信方法及び配信システムの実現に必要な要素技術に関する。

【0002】

【従来の技術】

デジタル技術の進展に伴い、あらゆるデジタルコンテンツ（文字データ（例えば、記号、図形）、オーディオデータ（例えば、音声、音楽）、ビデオデータ（例えば、静止画、動画）、オーディオデータとビデオデータの複合データ（例えば、映画、放送番組）、プログラムデータ、データベースデータその他のデジタルデータ）がネットワークや記録媒体を通じて配信されようとしている。

【0003】

【発明が解決しようとする課題】

一方、デジタルコンテンツは完全な複製物を容易に作成できるため、不正行為（例えば、不正復号再生、不正複製、横流し）が行われると、非常に大きな損害が生じるものと予測される。このため、不正行為からコンテンツ提供者（コンテンツ制作者や配信事業者）を保護する仕組み作りが急がれている。特に、制作に膨大な費用と人手を要し、資産価値の高いコンテンツ（例えば、映画）に関しては、不正行為によって莫大な損害が生じるため、不正行為が著しく困難な仕組み作りが求められる。

【0004】

しかし、防御能力が高いものは多大な設備投資を必要としたり、設備投資が比較的少なくて済むものは防御能力に問題がある等、コンテンツ提供者と受け手の

双方が納得できるような仕組みは確立されていないのが現状である。

【 0 0 0 5 】

例えば、不正行為に対する耐性を高く保ち続けたり、より再現性の高い出力技術が現れた場合には適宜最新の技術を導入できることが望ましいが、現在提案されているビジネスモデルでは受け手側に必要な機能を全て出力装置内に設ける構成を採るため、技術寿命の短いものに合わせて出力装置自体の買い替えが必要となる。しかし、出力装置の短期間での買い替えを前提とするビジネスモデルでは、受け手側の理解を得ることができない。またその結果として、陳腐化した技術の置き換えが進み難く、デジタルコンテンツが不正行為にあう危険性が高まるという弊害がある。

【 0 0 0 6 】

このため、資産価値の高いコンテンツの提供がコンテンツ制作者に認められなかったり、ビジネスモデル自体が受け手側に受け入れられず、システムの運用を開始できない等の問題が生じている。

【 0 0 0 7 】

本願明細書は以上の課題を考慮し、デジタルコンテンツの配信段階から最終出力段階に至るまで不正行為が極めて難しく、しかも合理的な対価によって長期にわたって高い防御機能を維持できる配信方法及び当該方法を適用したシステム並びにそれらを実現する要素技術について提案する。

【 0 0 0 8 】

【課題を解決するための手段】

かかる課題を解決するため以下の手段を提案する。

【 0 0 0 9 】

(1) 本願明細書で想定する配信モデル

以下の各手段では後述する処理を実行する上流側システムと下流側システムとで構成される配信モデルを想定する。

【 0 0 1 0 】

上流側システムが、デジタルコンテンツ毎に固有の暗号処理を施し、すなわちデジタルコンテンツ毎に固有の暗号鍵でデジタルコンテンツを暗号化し、

放送形式又は記録媒体の形態で下流側システムに配信を行う。このようにコンテンツに固有の暗号鍵を用いることにより、不正行為が行われてもその被害がコンテンツ単位でしか生じないようにする。

【 0 0 1 1 】

また、上流側システムは、デジタルコンテンツの暗号化に使用した暗号鍵の配信に際し、基本的に以下の２種類の方法のいずれかによって作成した配信先に固有の複数の鍵情報を、デジタルコンテンツとは別の配信経路（媒体を物理的に異にするもの、又は、配信時間帯を異にするもの。以下同じ。）であって、鍵情報相互間においても別の配信経路となるものを通じて対応する下流側システムに配信する。すなわち、鍵情報を複数の経路を通じて配信することにより、いずれかの経路を通じて配信される鍵情報が盗まれた場合でも、他の全ての鍵情報が盗まれない限り被害の発生を防止できる。なお配信される鍵情報は、暗号鍵そのものだけでなく、その発生情報（例えば、乱数）でもよい。また鍵情報は、暗号鍵を分割した合わせ鍵や部分鍵でもよい。

【 0 0 1 2 】

因みに上述の２種類の方法は、

- １）暗号鍵を配信先毎に固有の分割パターンで分割し、一組の部分鍵を生成する方法
 - ２）配信先毎に固有の異なる暗号鍵（請求項における第２の暗号鍵）を生成すると共に、当該暗号鍵でデジタルコンテンツの暗号化に使用した暗号鍵（請求項における第１の暗号鍵）を暗号したものを生成する方法
- の２つである。

【 0 0 1 3 】

ここでの配信先毎に固有の分割パターンや配信先毎に固有の異なる暗号鍵は、配信者毎に普遍的に割り当てられている場合もあれば、コンテンツ毎にその都度割り当てられる場合もある。勿論、不正行為対策の観点からは後者が望ましい。

【 0 0 1 4 】

一方、下流側システムは、複数の鍵情報から復元した暗号鍵でデジタルコンテンツに施されている暗号処理を解除する処理と、これにスクランブル処理を施

す処理を復号サーバで実行し、スクランブル処理の施されたデジタルコンテンツを出力装置に対して出力する。

【 0 0 1 5 】

このように暗号処理の復号機能を出力装置とは別に設けるようにしたことにより、受け手側にとって設備の更新負担が少なくて済むシステム構成とできる。すなわち、配信システムの運用開始後に暗号方式の変更を行う場合にも、復号サーバだけを更新すればよく、暗号処理の復号とは関係のない出力装置については性能に支障のない限りそのまま使用できるようになる。同様に、出力装置をより性能の高いものに置き換える場合でも何らの問題のない復号サーバについてはそのまま使用できるようになる。かかる仕組みは長期的な運用コストを低減する上で効果的である。

【 0 0 1 6 】

もっとも、単に復号機能と出力装置とを分離したのでは不正行為に対して極めて無防備な配信モデルとなってしまうが、復号サーバと出力装置との間を流れるのはスクランブル処理されたデジタルコンテンツであるので、復号サーバと出力装置の間でデジタルコンテンツを不正複製することはできないようになっている。

【 0 0 1 7 】

なお、復号サーバや出力装置においても不正行為の起こり得ない仕組みを採用する。例えば、正規の手続き以外では復号サーバや出力サーバの筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。また、復号サーバにおいて実行される特定の処理機能を集積回路化して処理の過程で現れる暗号鍵や生のデジタルコンテンツが取り出されないようにする仕組みを採用する。ここで正規の手続きとしては、例えば開封する資格を有する者のみが保持する電子的な鍵や物理的な鍵を使用することが考えられる。また、不正に開封する行為としては、例えば筐体を破壊することが考えられる。

【 0 0 1 8 】

(2) 配信モデルを実現する代表的な手段

以下、配信モデルを実現する代表的な手段について説明する。ここでの配信モ

デルは、前述のように上流側システムと下流側システムとで構成される配信システムを前提とする。また以下では、配信モデル全体からみた配信方法について説明する。

【 0 0 1 9 】

なお、各手段の上流側システムで実行される各処理は、上流側システムを構成する制作者システム及び配信者システムのいずれかで行われる。処理機能どのように振り分けるかはビジネス上の選択による。従って、制作者システムと配信者システムの具体的なハードウェア構成やソフトウェア構成は種々のものが考えられる。例えば、デジタルコンテンツを暗号化するまでの処理と各配信先に応じた複数の鍵情報を生成する処理については制作者システムで行われるようにすると、暗号鍵（マスター鍵）を知り得るのはコンテンツ制作者のみとなるため、コンテンツ制作者にとって秘匿性を保持し易い処理方法となる。

【 0 0 2 0 】

以下の手段では、電子透かしについて言及していないが、不正行為の防止や流出経路の特定の観点からはデジタルコンテンツを暗号化する前に、固有の電子透かしを入れておくことが望ましい。

【 0 0 2 1 】

また、暗号化されたデジタルコンテンツの配信に際し、配信事業者や伝送網の管理者が別途他の暗号処理を施すことは自由である。また、鍵情報を配信する場合にも、実際にはデジタル証明書等によって相手先が真正な配信先であることを確認した上で相手方の公開鍵で鍵情報を暗号化しておくことが安全を期する上で望ましい。

【 0 0 2 2 】

なお以下の手段では、分割処理によって暗号鍵から直接得られる鍵を「合わせ鍵」と、合わせ鍵を更に分割することで得られる鍵を「部分鍵」というものとする。もっとも、いずれの鍵も暗号鍵の一部分である点では同じである。また以下の手段では、暗号鍵を暗号化するのに使用する鍵を「多重鍵」というものとする。

【 0 0 2 3 】

また各手段において鍵情報を配信する場合には、鍵情報の伝送網に、デジタルコンテンツの伝送網と物理的に同じものを用いることも可能である。ただし、その場合にはデジタルコンテンツと鍵情報を同時刻に配信することはせず、それぞれの配信時間帯をずらし、實際上、別経路で配信するのと同様の状態で配信を行うことが望ましい。これは、デジタルコンテンツと鍵情報を同一の伝送網を通じて同時配信すると、1回の不正行為でデジタルコンテンツと鍵情報の一部を同時に入手できるため、その分、デジタルコンテンツに施されている暗号が解除される危険性が高まるためである。

【 0 0 2 4 】

(2 - 1) 第 1 の手段

第 1 の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。なお、上流側システムは、デジタルコンテンツを供給する制作者システムと、供給を受けたデジタルコンテンツの配信を実行する配信者システムとで構成される複合システムである。また、下流側システムは、デジタルコンテンツに施されている暗号処理を解除する復号サーバと、デジタルコンテンツを所定の出力形態で再生する出力装置とで構成される複合システムである。これは他の手段でも同様である。

【 0 0 2 5 】

上流側システムが、各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 0 2 6 】

また、下流側システムの復号サーバが、伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と記録媒体の形態で配信を受けた残りの部分とを基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号

鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 0 2 7 】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【 0 0 2 8 】

第 1 の手段は要するに、デジタルコンテンツの暗号化に使用した暗号鍵を、各配信先（下流側システム）に固有の分割規則で分割して一組の合わせ鍵を生成し、その一部を伝送網を通じて配信し、残りを記録媒体の形態で配信する配信方式と、配信を受けた鍵情報から復元された暗号鍵を用い暗号処理の解除されたデジタルコンテンツにスクランブル処理を施し出力装置に出力する再生方式とを組み合わせたものである。

【 0 0 2 9 】

ここで、合わせ鍵の配信に使用する記録媒体には、磁気読み取り方式の媒体（例えば、磁気テープ、フロッピーディスク、磁気カード）、光学読み取り方式の媒体（例えば、CD-ROM、MO、CD-R、DVD）、半導体メモリ（メモリカード（矩形型、正方形型など形状は問わない。）、ICカード）その他が考えられる。当該記録媒体の配信には、郵便制度や宅配制度を使用する。現行の制度では、秘匿性の観点から書留郵便の使用を想定する。この配信用の記録媒体についての記載は以下の各手段についても共通である。

【 0 0 3 0 】

また、合わせ鍵の配信に使用する伝送網は、デジタルコンテンツを伝送網を介して伝送する場合、基本的にはデジタルコンテンツと別のものを使用する。ただし、両者を同じ伝送網を使って配信することも可能である。なお、両者を同じ伝送網を通じて伝送する場合には、合わせ鍵の伝送とデジタルコンテンツの伝送とは時間的に別の時間帯に行うことが不正行為に対する対抗上望ましい。これらの記載も、後述する各手段に現れる部分鍵や多重鍵の配信に共通する。

【 0 0 3 1 】

また、復号サーバで生成するスクランブル鍵とスクランブル解除鍵は、同じデジタルコンテンツについては同じであってもよいし、暗号処理を解除する毎に固有の鍵を発生するようにしてもよい。不正行為に対する対策としては後者の方が望ましい。

【 0 0 3 2 】

また、出力装置としては表示装置（例えば、モニタ装置、テレビジョン受像機、プロジェクタ装置、携帯型の電子機器）、印刷装置、スピーカ、記録媒体への記録装置等が考えられる。

【 0 0 3 3 】

ここで、出力装置における所定の出力形態には、デジタルコンテンツが例えばビデオデータであれば、表示画面への表示、投影面への投影が考えられる。またデジタルコンテンツが例えばオーディオデータであれば、スピーカを通じての再生が考えられる。勿論、オーディオデータとビデオデータの複合データであれば、その同時に2つの出力が行われる。

【 0 0 3 4 】

なお、この第1の手段では信号処理の観点から説明しているが、これらの処理機能を備えるハードウェア構成によって実現することも可能であるし、同様の機能をソフトウェア処理として実現することも可能である。後述する他の手段についても同様である。この場合、ハードウェアやソフトウェア（コンピュータに該当処理を実行させるプログラムを記録した記録媒体）は上流側システムと下流側システムのそれぞれについて用意する。ハードウェアには、復号サーバや出力装

置といった完成品の他、インタフェースボードや半導体集積回路等といった構成部品（請求項における回路装置）が考えられる。

【 0 0 3 5 】

かかる手段を用いることにより、たとえ複数の経路で配信される鍵情報のうちいずれかが盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、鍵情報をデジタルコンテンツとは別の経路（上述のように同一の経路を用いながら時間的に別の時間帯に配信する場合を含む。）で配信する場合には、鍵情報の一部を盗んだ不正行為者が暗号化されたデジタルコンテンツをも入手した場合でも、暗号鍵の復元に必要な鍵情報はデジタルコンテンツとは別に配信されるため、生のデジタルコンテンツが復号化される事態を確実に回避できる。

【 0 0 3 6 】

また、暗号処理が解除されたデジタルコンテンツにスクランブル処理を施す方式を採用したことにより、不正行為に対する十分な防御能力を保持したままで復号機能を実行するサーバ装置と再生機能を実行する出力装置との分離を実現できる。すなわち、十分な対不正行為能力と経済性とを兼ね備えた配信モデルを提供できる。

【 0 0 3 7 】

（ 2 - 2 ） 第 2 の 手 段

第 2 の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 0 3 8 】

上流側システムが、各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第 1 の伝送網を通じて各特定者に配信する処理と、生成された部分鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残

りの合わせ鍵又はその発生情報を第2の伝送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【0039】

また、下流側システムの復号サーバが、第1の伝送網を通じて配信を受けた部分鍵又はその発生情報と、記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第2の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理の解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【0040】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【0041】

第2の手段は要するに、デジタルコンテンツの暗号化に使用した暗号鍵を、各配信先（下流側システム）に固有の分割規則で分割して一組の合わせ鍵を生成し、その一部はそのまま第1の伝送網を通じて配信するものの、残る合わせ鍵については更に所定の分割規則で分割し、生成された一組の部分鍵の一部を第2の伝送網を通じて配信し、残りは記録媒体の形態で配信する方式を採用するものであり、この点で第1の手段と異なっている。

【 0 0 4 2 】

すなわち、鍵情報の配信を2つの伝送網（異なる伝送網を用いる場合と、同一伝送網に異なる時点で鍵情報を配信する場合とがある。）と記録媒体とで実現する点で異なるものである。

【 0 0 4 3 】

ここで、合わせ鍵から一組の部分鍵を生成するのに用いる分割規則は、全ての配信先に共通の規則でもよいし、各配信先に固有の規則でもよいし、特定地域その他の条件で区分された配信先の集合毎に固有の規則でもよい。他の手段においても同様である。

【 0 0 4 4 】

かかる手段を用いる場合には、第1の手段よりも更に鍵情報の配信経路が増えるため、伝送経路上での不正行為により高い耐性を有する配信モデルを提供できる。

【 0 0 4 5 】

なおここでは、合わせ鍵の一部を更に分割して配信用の鍵情報を生成しているがこれに代え、多重鍵で暗号化する方式を採用することもできる。かかる変形例は、同様の仕組みを採用する他の手段についても同様である。

【 0 0 4 6 】

(2 - 3) 第 3 の 手 段

第3の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 0 4 7 】

上流側システムが、各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第1の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残りの合わせ鍵又は

その発生情報を記録媒体の形態での配信用に鍵専用の第2の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 0 4 8 】

また、下流側システムの復号サーバが、第1の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第2の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、記録媒体の形態で配信を受けた合わせ鍵又はその発生情報を基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 0 4 9 】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【 0 0 5 0 】

第3の手段は要するに、第2の手段では第2の伝送網を介して配信した合わせ鍵を記録媒体の形態で配信する方式を採用するものである。すなわち、鍵情報の配信を1つの伝送網と2つの記録媒体とで実現するものである。勿論、2つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっても構わない。

【 0 0 5 1 】

かかる手段も、第 1 の手段に加えて更に鍵情報の配信経路が増えるため、より不正行為に対する安全性の高い配信モデルを提供できる。また、伝送網を通じた配信に比して盗難を早期に発見し易いため、暗号鍵の変更等の対抗策を採り易いという効果が期待できる。

【 0 0 5 2 】

(2 - 4) 第 4 の手段

第 4 の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 0 5 3 】

上流側システムが、各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を第 1 の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を第 2 の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 0 5 4 】

また、下流側システムの復号サーバが、第 1 の伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と、第 2 の伝送網を通じて配信を受けたそれらと対をなす残りの部分とを基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理において生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 0 5 5 】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【 0 0 5 6 】

第4の手段は要するに、第1の手段では記録媒体を使用して配信した合わせ鍵を伝送網を用いて配信する方式を採用するものである。すなわち、鍵情報の配信を2つの伝送網を用いて実現するものである。ここでの配信も、異なる2つの伝送網を用いて配信する場合と、同一の伝送網を用いながら異なる時点に鍵情報を配信することで等価的に2つの伝送網を用いた配信とする場合が考えられる。なお、この手段の場合には、成りすましによる暗号鍵の搾取の可能性があるため、鍵情報の配信に際してはデジタル証明書を使用した本人確認と配信先が公開する公開鍵を用いた鍵暗号の処理を行うことが望ましい。

【 0 0 5 7 】

かかる手段を用いることにより、全ての鍵情報を即時性に優れた伝送網を通じて配信することになるので、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からデジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。勿論、鍵情報をデジタルコンテンツとは別の経路で配信する場合（すなわち、物理的に別媒体を用いて配信する場合か、同一媒体であっても時間的に異なる時点に配信する場合）には、鍵情報の一部と暗号化されたデジタルコンテンツを盗んでも生のデジタルコンテンツを復号化することはできない。

【 0 0 5 8 】

(2 - 5) 第5の手段

第5の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 0 5 9 】

上流側システムが、各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配

信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を記録媒体の形態での配信用に鍵専用の第1の記録媒体に書き込む処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の第2の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【0060】

また、下流側システムの復号サーバが、第1の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報の一部と、第2の記録媒体の形態で配信を受けたそれらと対をなす残りの部分とを基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【0061】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【0062】

第5の手段は要するに、第1の手段では伝送網を介して配信した合わせ鍵を記録媒体の形態で配信する方式を採用するものである。すなわち、鍵情報の配信を2つとも記録媒体の形態で実現するものである。この場合も、2つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り

方式については同じでも、異なっても構わない。

【 0 0 6 3 】

かかる手段を用いる場合には、伝送網を通じた配信に比して盗難を早期に発見し易いため、暗号鍵の変更等の対策を採り易くデジタルコンテンツの盗難の起こり難いという効果が期待できる。

【 0 0 6 4 】

(2 - 6) 第 6 の手段

第 6 の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 0 6 5 】

上流側システムが、各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第 1 の伝送網を通じて各特定者に配信する処理と、残る部分鍵又はその発生情報を第 2 の伝送網を通じて各特定者に配信する処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を第 3 の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 0 6 6 】

また、下流側システムの復号サーバが、第 1 の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第 2 の伝送網を通じて配信を受けた残りの部分鍵又はその発生情報と、第 3 の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツ

に施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 0 6 7 】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【 0 0 6 8 】

第6の手段は要するに、第2の手段では記録媒体を用いて配信していた部分鍵を伝送網を介して配信する方式を採用するものである。すなわち、3つの鍵情報の全てを伝送網を通じて配信するものである。なお、この手段の場合には、成りすましによる暗号鍵の搾取の可能性があるため、鍵情報の配信に際してはデジタル証明書を使用した本人確認と配信先が公開する公開鍵を用いた鍵暗号の処理を行うことが望ましい。

【 0 0 6 9 】

この手段の場合、全ての鍵情報を即時性に優れた伝送網を通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合に比して鍵の配信からデジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。勿論、鍵情報をデジタルコンテンツとは別の経路で配信する場合（すなわち、物理的に別媒体を用いて配信する場合か、同一媒体であっても時間的に異なる時点に配信する場合）には、鍵情報の一部と暗号化されたデジタルコンテンツを盗んでも生のデジタルコンテンツを復号化することはできない。

【 0 0 7 0 】

(2 - 7) 第7の手段

第7の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 0 7 1 】

上流側システムが、各デジタルコンテンツに固有の暗号鍵を発生する処理と、デジタルコンテンツを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第 1 の記録媒体に書き込む処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第 2 の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第 3 の記録媒体に記録する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 0 7 2 】

また、下流側システムの復号サーバが、第 1 の記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第 2 の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第 3 の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報とを基に対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 0 7 3 】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを

所定の出力形態で再生する処理とを実行するものを提案する。

【 0 0 7 4 】

第 7 の手段は要するに、第 3 の手段では伝送媒体を介して配信していた部分鍵を記録媒体を用いて配信する方式を採用するものである。すなわち、3 つの鍵情報の全てを記録媒体を用いて配信するものである。この場合も、3 つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっても構わない。

【 0 0 7 5 】

かかる手段を用いる場合には、伝送網を通じた配信に比して盗難を早期に発見し易いため、暗号鍵の変更等の対策を採り易くデジタルコンテンツの盗難の起こり難いという効果が期待できる。

【 0 0 7 6 】

(2 - 8) 第 8 の手段

第 8 の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 0 7 7 】

上流側システムが、各デジタルコンテンツに固有の第 1 の暗号鍵を発生する処理と、デジタルコンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、第 2 の暗号鍵によって第 1 の暗号鍵又はその発生情報を暗号化し、伝送網を通じて特定者に配信する処理と、第 2 の暗号鍵を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 0 7 8 】

また、下流側システムの復号サーバが、記録媒体の形態で配信を受けた第 2 の暗号鍵又はその発生情報を基に、伝送網を通じて配信を受けた第 1 の暗号鍵又はその発生情報に施されている暗号処理を解除して、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタ

ルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 0 7 9 】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【 0 0 8 0 】

第 8 の手段は要するに、配信先（下流側システム）毎に固有の第 2 の暗号鍵であって、暗号化するデジタルコンテンツに固有なもので暗号化した第 1 の暗号鍵を伝送網を通じて配信し、その暗号化に使用した第 2 の暗号鍵を記録媒体の形態で配信する方式を採用するものである。この手段は、配信される鍵情報の発生の仕方が第 1 の手段と異なるだけで、配信の仕方自体は第 1 の手段の場合と同じである。

【 0 0 8 1 】

かかる手段を用いることにより、たとえ複数の経路で配信される鍵情報のうちいずれかが盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、鍵情報をデジタルコンテンツとは別の経路（上述のように同一の経路を用いながら時間的に別の時点に配信する場合を含む。）で配信する場合には、鍵情報の一部を盗んだ不正行為者が暗号化されたデジタルコンテンツをも入手した場合でも、暗号鍵の復元に必要な鍵情報はデジタルコンテンツとは別に配信されるため、生のデジタルコンテンツが復号化さ

れる事態を確実に回避できる。

【 0 0 8 2 】

また記録媒体として配信される第 2 の暗号鍵が盗まれた場合でも当該鍵はデジタルコンテンツに固有なものであるため、同じ配信者にそれ以後配信されるデジタルコンテンツの解除には使用することができず、被害の継続的発生を確実に防止できる。

【 0 0 8 3 】

(2 - 9) 第 9 の手段

第 9 の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 0 8 4 】

上流側システムが、各デジタルコンテンツに固有の第 1 の暗号鍵を発生する処理と、デジタルコンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、第 2 の暗号鍵によって第 1 の暗号鍵又はその発生情報を暗号化し、第 1 の伝送網を通じて特定者に配信する処理と、第 2 の暗号鍵を基に配信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第 2 の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 0 8 5 】

また、下流側システムの復号サーバが、第 2 の伝送網を通じて配信を受けた合わせ鍵の一部と、記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第 2 の暗号鍵を復元して、第 1 の伝送網を通じて配信を受けた第 1 の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所

的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 0 8 6 】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【 0 0 8 7 】

第 9 の手段は要するに、第 8 の手段では記録媒体の形態で配信した配信先に固有の暗号鍵を所定の分割規則で分割し、生成された一組の合わせ鍵の一部を伝送網を通じて配信し、残りは記録媒体の形態で配信する方式を採用するものである。すなわち、第 9 の手段では、配信先に固有の暗号鍵がそのままの状態配信されるのを回避するものである。

【 0 0 8 8 】

なお当該手段における配信は、全体的にみると、鍵情報の伝送を 2 つの伝送網（異なる伝送網を用いる場合と、同一伝送網に異なる時点で鍵情報を配信する場合とがある。）と記録媒体とで実現するものである。

【 0 0 8 9 】

ここで、配信先に固有の暗号鍵から一組の合わせ鍵を生成するのに用いる分割規則は、全ての配信先に共通の規則でもよいし、各配信先に固有の規則でもよいし、特定地域その他の条件で区分された配信先の集合毎に固有の規則でもよい。

【 0 0 9 0 】

かかる手段では、第 8 の手段と異なり、各配信先に固有の暗号鍵がそのままの状態（記録媒体の中ではあるが）配信されないため、記録媒体の盗難だけでは多重鍵を入手することはできず、その分、デジタルコンテンツの不正復号を困

難にできる。

【 0 0 9 1 】

(2 - 1 0) 第 1 0 の手段

第 1 0 の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 0 9 2 】

上流側システムが、各デジタルコンテンツに固有の第 1 の暗号鍵を発生する処理と、デジタルコンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、第 2 の暗号鍵によって暗号化された第 1 の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第 1 の記録媒体に書き込む処理と、第 2 の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第 2 の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 0 9 3 】

また、下流側システムの復号サーバが、伝送網を通じて配信を受けた合わせ鍵の一部と、第 2 の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第 2 の暗号鍵を復元して、第 1 の記録媒体を通じて配信を受けた第 1 の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先であって、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタ

ルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 0 9 4 】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【 0 0 9 5 】

第 1 0 の手段は要するに、第 9 の手段では第 1 の伝送網を介して配信されていたデジタルコンテンツ用の暗号鍵を記録媒体の形態で配信する方式を採用するものである。すなわち、鍵情報の配信を 1 つの伝送網と 2 つの記録媒体とで実現するものである。勿論、2 つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっているものでも構わない。

【 0 0 9 6 】

かかる手段の場合には、暗号化された暗号鍵が記録媒体を通じて配信される分、当該鍵を伝送網を通じて配信する場合に比して盗難の早期発見を可能とでき、暗号鍵の変更等の対策を採り易いという効果を期待できる。

【 0 0 9 7 】

(2 - 1 1) 第 1 1 の手段

第 1 1 の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 0 9 8 】

上流側システムが、各デジタルコンテンツに固有の第 1 の暗号鍵を発生する処理と、デジタルコンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、第 2 の暗号鍵によって第 1 の暗号鍵又はその発生情報を暗号化し、第 1 の伝送網を通じて特定者に配信する処理と、第 2 の暗号鍵を第 2 の伝

送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 0 9 9 】

また、下流側システムの復号サーバが、第 2 の伝送網を通じて配信を受けた第 2 の暗号鍵又はその発生情報を基に、第 1 の伝送網を通じて配信を受けた第 1 の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 1 0 0 】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【 0 1 0 1 】

第 1 1 の手段は要するに、第 8 の手段では記録媒体を用いて配信した第 2 の暗号鍵を伝送網を通じて配信する方式を採用するものである。すなわち、鍵情報の配信を 2 つの伝送網を用いて実現するものである。この手段は、配信される鍵情報の発生の方が第 4 の手段と異なるだけで、配信の仕方自体は第 4 の手段の場合と同じである。

【 0 1 0 2 】

かかる手段を用いることにより、たとえば複数の経路で配信される鍵情報のうち

いずれかが盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、鍵情報をデジタルコンテンツとは別の経路（上述のように同一の経路を用いながら時間的に別の時点に配信する場合を含む。）で配信する場合には、鍵情報の一部を盗んだ不正行為者が暗号化されたデジタルコンテンツをも入手した場合でも、暗号鍵の復元に必要な鍵情報はデジタルコンテンツとは別に配信されるため、生のデジタルコンテンツが復号化される事態を確実に回避できる。

【 0 1 0 3 】

（ 2 - 1 2 ） 第 1 2 の 手 段

第 1 2 の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 1 0 4 】

上流側システムが、各デジタルコンテンツに固有の第 1 の暗号鍵を発生する処理と、デジタルコンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、第 2 の暗号鍵によって第 1 の暗号鍵又はその発生情報を暗号化し、記録媒体の形態での配信用に鍵専用の第 1 の記録媒体に書き込む処理と、第 2 の暗号鍵を記録媒体の形態での配信用に鍵専用の第 2 の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 1 0 5 】

また、下流側システムの復号サーバが、第 2 の記録媒体の形態で配信を受けた第 2 の暗号鍵又はその発生情報を基に、第 1 の記録媒体の形態で配信を受けた第 1 の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化

処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 1 0 6 】

下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【 0 1 0 7 】

第 1 2 の手段は要するに、第 8 の手段では伝送媒体を介して配信した暗号化済みの第 1 の暗号鍵を記録媒体の形態で配信する方式を採用するものである。すなわち、鍵情報の配信を 2 つとも記録媒体の形態で実現するものである。この手段は、配信される鍵情報の発生の仕方が第 5 の手段と異なるだけで、配信の仕方自体は第 5 の手段の場合と同じである。

【 0 1 0 8 】

かかる手段を用いる場合には、伝送網を通じた配信に比して盗難を早期に発見し易いため、暗号鍵の変更等の対策を採り易くデジタルコンテンツの盗難の起こり難いという効果が期待できる。

【 0 1 0 9 】

(2 - 1 3) 第 1 3 の手段

第 1 3 の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 1 1 0 】

上流側システムが、各デジタルコンテンツに固有の第 1 の暗号鍵を発生する処理と、デジタルコンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、第 2 の暗号鍵によって第 1 の暗号鍵又はその発生情報を暗号

化し、第 1 の伝送網を通じて特定者に配信する処理と、第 2 の暗号鍵を基に配信先である各特定者に固有の一组の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第 2 の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を第 3 の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 1 1 1 】

また、下流側システムの復号サーバが、第 2 の伝送網を通じて配信を受けた合わせ鍵の一部と、第 3 の伝送網を通じて配信を受けた合わせ鍵の残りの部分とから第 2 の暗号鍵を復元して、第 1 の伝送網を通じて配信を受けた第 1 の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 1 1 2 】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【 0 1 1 3 】

第 1 3 の手段は要するに、第 9 の手段では記録媒体を用いて配信していた部分鍵を伝送網を介して配信する方式を採用するものである。すなわち、3 つの鍵情

報の全てを伝送網を通じて配信するものである。なお、この手段の場合には、成りすましによる暗号鍵の搾取の可能性があるため、鍵情報の配信に際してはデジタル証明書を使用した本人確認と配信先が公開する公開鍵を用いた鍵暗号の処理を行うことが望ましい。

【 0 1 1 4 】

この手段の場合、全ての鍵情報を即時性に優れた伝送網を通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合に比して鍵の配信からデジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。勿論、鍵情報をデジタルコンテンツとは別の経路で配信する場合（すなわち、物理的に別媒体を用いて配信する場合か、同一媒体であっても時間的に異なる時点に配信する場合）には、鍵情報の一部と暗号化されたデジタルコンテンツを盗んでも生のデジタルコンテンツを復号化することはできない。

【 0 1 1 5 】

（ 2 - 1 4 ） 第 1 4 の 手 段

第 1 4 の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【 0 1 1 6 】

上流側システムが、各デジタルコンテンツに固有の第 1 の暗号鍵を発生する処理と、デジタルコンテンツを第 1 の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第 2 の暗号鍵であって、デジタルコンテンツに固有のものを発生する処理と、第 2 の暗号鍵によって暗号化された第 1 の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第 1 の記録媒体に書き込む処理と、第 2 の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第 2 の記録媒体に書き込む処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第 3 の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたデジタルコンテンツを配信する処理とを実行するものを提案する。

【 0 1 1 7 】

また、下流側システムの復号サーバが、第2の記録媒体を通じて配信を受けた合わせ鍵の一部と、第3の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第2の暗号鍵を復元して、第1の記録媒体を通じて配信を受けた第1の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するデジタルコンテンツに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するデジタルコンテンツに施されている暗号処理を解除する処理と、デジタルコンテンツに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツに施されている符号化処理を復号化し、デジタルコンテンツを復元する処理と、復元されたデジタルコンテンツの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、デジタルコンテンツをスクランブル処理して出力する処理とを実行するものを提案する。

【 0 1 1 8 】

また、下流側システムの出力装置が、復号サーバから入力されるデジタルコンテンツに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたデジタルコンテンツの唯一の出力先において、当該デジタルコンテンツを所定の出力形態で再生する処理とを実行するものを提案する。

【 0 1 1 9 】

第14の手段は要するに、第10の手段では伝送媒体を介して配信していた部分鍵を記録媒体を用いて配信する方式を採用するものである。すなわち、3つの鍵情報の全てを記録媒体を用いて配信するものである。この場合も、3つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっているものでも構わない。

【 0 1 2 0 】

かかる手段を用いる場合には、伝送網を通じた配信に比して盗難を早期に発見し易いため、暗号鍵の変更等の対策を採り易くデジタルコンテンツの盗難の起こり難いという効果が期待できる。

【 0 1 2 1 】

【発明の実施の形態】

(1) ビジネスモデル

(1 - 1) 一般例

図 1 に本願明細書が想定するビジネスモデルの一般構成例を示す。このビジネスモデルは、デジタルコンテンツの配信者と、デジタルコンテンツの受け手である特定者とから構成される。配信者はコンテンツ制作会社 1 と電子配信事業者 2 で構成される。特定者 6 及び 7 は個人宅や事業者で構成される。

【 0 1 2 2 】

なお、コンテンツ制作会社内のシステムと電子配信事業者内のシステムとが配信システムにおける上流側システムを構成し、特定者内のシステムが配信システムにおける下流側システムを構成する。

【 0 1 2 3 】

配信対象に想定するデジタルコンテンツは、文字データ（例えば、記号、図形）、オーディオデータ（例えば、音声、音楽）、ビデオデータ（例えば、静止画、動画）、オーディオデータとビデオデータの複合データ（例えば、映画、放送番組）、プログラムデータ、データベースデータ、その他のデジタルデータがある。

【 0 1 2 4 】

一般に、デジタルコンテンツの配信には、伝送帯域が広く大容量のデータを配信するのに適した高速配信用ネットワーク 3 を想定する（図 1）。ただし、CD-ROM や DVD その他の記録媒体による形態での配信を排除するものではない。高速配信用ネットワーク 3 には、放送衛星や光ファイバその他の広帯域伝送網を使用する。これらは少なくとも下り方向について大容量の伝送が可能なものを使用する。もっとも、上り方向への伝送も可能な双方向伝送網を用いてもよい。

【 0 1 2 5 】

高速配信用ネットワーク 3 には、図 2 に示したようなデータ構造のデータ 8 が配信される。ここで、図 1 のデータ 8 には鍵の絵 8 A を表しているが、これはネ

ットワーク提供事業者が独自に掛けた鍵を表している。

【 0 1 2 6 】

勿論、ここでの鍵は暗号処理のことである。これらの鍵が掛けられないこともある。デジタルコンテンツの不正行為に対する安全性を最優先するコンテンツ制作会社 1 や電子配信事業者 2 は、ネットワーク上でも独自にデータに暗号処理を施すネットワーク事業者を選択するであろうし、その中でもより安全性の高い暗号処理を実行するネットワーク事業者を選択するものと考えられる。

【 0 1 2 7 】

破線で囲まれた中身の部分が電子配信事業者 2 から出力されるデータに相当する。図 2 の場合、当該データには、データ又はファイルの格納情報を示すファイルアロケーションテーブル (F A T : File Allocation Table) 8 B と、デジタルコンテンツの使用条件 (配信先、配信先毎の再生可能期間及び再生回数その他の条件) を含む業務データ 8 C と、映像データ 8 D と、音声データ 8 E とが格納されている。

【 0 1 2 8 】

これら各データに掛けられている鍵の絵は、コンテンツ制作者 1 又は電子配信事業者 2 のいずれかのシステムにおいて、又はその双方のシステムにおいて各コンテンツに固有の鍵が掛けられていることを表している。

【 0 1 2 9 】

映像データ 8 D には、異なる符号化復号化方式 (コーデック) で符号化された複数種類のデジタル映像コンテンツが格納される。図 1 では、3 種類のコーデックに対応するデジタルコンテンツが格納されている状態を表している。例えば、M P E G (Moving Picture Experts Group)、W a v e l e t その他がある。

【 0 1 3 0 】

このようにデジタル映像コンテンツを複数種類のコーデック方式で符号化し配信するのは、特定者側のシステム構成に自由度をもたせるためである。すなわち、特定者側に単一コーデックのシステム構成を強制するのではなく、各自に都合のよいコーデックを選択可能とするためである。

【 0 1 3 1 】

音声データ 8 E についても同様である。図 2 の場合、2 種類のコーデック方式で符号化されたデータが格納されている。例えば、M P E G その他がある。

【 0 1 3 2 】

図 1 の場合、特定者 A と表した個人宅が必要とするデータは、映像コーデック 1 と音声コーデック 1 であるため、それらが配信を受けたデータの中から F A T の情報を基に選択的に受信される又は再生される。同様に、特定者 B と表した事業者が必要とするデータは、映像コーデック 2 と音声コーデック 2 であるため、それらが配信を受けたデータの中から F A T の情報を基に選択的に受信される又は再生される。

【 0 1 3 3 】

以上が高速配信用ネットワーク 3 を介して配信を受けるデジタルコンテンツについての説明である。次に、当該デジタルコンテンツに施されている条件付きアクセス処理、すなわち暗号処理を解除するのに必要な暗号鍵の配信経路について説明する。図 1 における暗号鍵の配信経路は、広域ネットワーク（伝送媒体）4 と記録媒体 5 の 2 つである。共通鍵を復元するのに少なくとも 2 種類の鍵情報を必要とする場合において、その一部を広域ネットワーク 4 を介して電子的に配信し、残る一部を記録媒体 5 を通じて物理的に配信する方式を採用する。

【 0 1 3 4 】

なお、ここでの広域ネットワーク 4 は双方向通信が可能な伝送網を想定している。例えば、公衆網（例えば、インターネット網、A T M 網、パケット通信網）や専用線網が考えられる。また、記録媒体 5 は前述の課題を解決するための手段にて述べたように、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他を想定する。その配信に郵便制度や宅配制度を利用することも前述の通りである。

【 0 1 3 5 】

ここで、デジタルコンテンツに掛けられている暗号処理を解除するのに必要な鍵は全ての配信先について共通であるが、各配信先に個別に配信される鍵情報は、図 1 における特定者 A の鍵情報と特定者 B の鍵情報のように、各配信者毎に

固有なものを想定する。これはある特定者宛てに配信された全ての鍵情報を入手しなければ、デジタルコンテンツに掛けられている鍵を復元できないようにするためである。このような仕組みを採用することで、このビジネスモデルは、全ての鍵情報の入手がより困難なもの又は全ての鍵情報を入手するまでに時間を要するものとしている。なお時間がかかる分、鍵情報の盗難が発見された後、暗号鍵を変更する等の対策が可能となる。

【 0 1 3 6 】

ところで、デジタルコンテンツに掛けられる暗号鍵と各配信先に配信される鍵情報のそれぞれとしては、いずれも配信対象であるデジタルコンテンツに固有なものを使用する。これは、全ての鍵情報が不正に入手されてデジタルコンテンツの復号に成功されたとしても被害を当該デジタルコンテンツのみに限定するためである。

【 0 1 3 7 】

また、基本的に鍵情報の配信経路は、図 1 に示すように、ネットワークと記録媒体というように媒体を異にするもの想定する。これは以下の理由による。まず、ネットワークでの配信は即時に実行できるという利点を有するが、その一方で鍵情報が盗難されても発見が難しいという欠点がある。これに対し、記録媒体での配信は特定者が入手するまでに時間を要するという欠点を有するものの、鍵情報の盗難を物理的に確認することができ、盗難を発見し易いという利点がある。

【 0 1 3 8 】

そこで、本願明細書で想定する多くのビジネスモデルでは、ネットワークを介しての配信と、記録媒体による物理的な配信との組み合わせを想定する。もっとも以上は一般的な理由によるものであり、ネットワークを使った配信でも不正行為のおそれがない場合や困難な場合には、全ての鍵情報をネットワークを介して配信すればよい。また、鍵情報の配信からデジタルコンテンツの配信までに期間的な余裕がある場合には、鍵情報の全てを記録媒体を使用して配信することもできる。

【 0 1 3 9 】

因みに、デジタルコンテンツの暗号処理に使用する暗号技術については技術

的な制約はなく、出願当時知られている各種の技術は勿論のこと将来現れるであろう各種の技術についても適用できる。暗号方式を問わないため技術的な寿命の影響を受け難いビジネスモデルとできる。また、常に運用当時最高の技術を選択できるため、その分、不正行為に強いビジネスモデルとできる。

【0140】

また図1において広域ネットワーク4と記録媒体5との2つの経路を通じて配信される鍵情報は、課題を解決するための手段において説明したように、配信先毎に固有の分割パターンで分割された一組の合わせ鍵（部分鍵）の組、又は、配信先毎に発生された固有の多重鍵で暗号化された暗号鍵と多重鍵の組を一般には想定する。

【0141】

（1-2）具体例

図3に、具体的なビジネスモデル例を示す。これは映画コンテンツを電子的に配信するビジネスモデルについてのものである。この種のビジネスモデルは従来からその実現に向け各種のビジネスモデル案が提供されているが、映画コンテンツの事業者と配信を受ける劇場側の双方から未だ納得を得られておらず、実用に至ったものはない。そこで、本願明細書の配信モデルを適用することを考える。

【0142】

このビジネスモデルの場合、図1のコンテンツ制作会社1は映画製作会社になり、デジタルコンテンツの配信を受ける特定者は劇場A、Bに変わる。なお図3の場合、映画コンテンツに特有な構成として、映画製作会社1から提供されるフィルム画像を電子画像に変換する工程（テレシネ工程：Film to Video Conversion）aを表している。また図では区別していないが、劇場A、Bは大規模な映画館、小規模な映画館、いわゆるシネコンと呼ばれる映画館が想定される。

【0143】

（2）配信システム例

上述のビジネスモデルを実現する配信システムの機能ブロック構成例を示す。なお各システム例は、課題を解決するための手段で説明した第1～第14の各手段に対応する。

【 0 1 4 4 】

(2 - 1) 第 1 のシステム例

図 4 に、上述のビジネスモデルを実現するための第 1 のシステム例を示す。当該システムは上流側システムと下流側システムとで構成される。上流側システムは、コンテンツ制作会社 1 のシステムと電子配信事業者 2 のシステムの複合システムでなる。一方、下流側システムはデジタルコンテンツの配信を受ける特定者毎に固有のシステムでなる。

【 0 1 4 5 】

(2 - 1 - 1) システム構成

図 4 の場合、上流側システムは、コンテンツサーバ 1 1 と、コンテンツ符号化部 1 2 と、暗号化部 1 3 と、送出サーバ 1 4 と、コンテンツ管理サーバ 1 5 と、鍵発生部 1 6 と、配信先管理サーバ 1 7 と、合わせ鍵生成部 1 8 と、書込部 1 9 とから構成される。

【 0 1 4 6 】

図 4 では、上流側システムにおけるこれらの各構成要素がいずれの事業者内システムに設けられるかをあえて明示していないが、これは各構成要素を上流側システムと下流側システムとでどのように配分するかはビジネス上の選択となるためである。なお各構成要素の配分の仕方は、他のシステム例についても共通する事項であるため、後段の「各システムで想定される運用形態」の項で別途説明する。

【 0 1 4 7 】

一方、下流側システムは、受信サーバ 3 1 と、読取部 3 2 と、復号サーバ 3 3 と、出力装置 3 4 (デスクランブル部 3 4 A) とから構成される。このうち、復号サーバ 3 3 は、更に復号機能部 3 5 (復号化部 3 5 A、鍵復元部 3 5 B、コンテンツ復号化部 3 5 C、スクランブル部 3 5 D) と、スクランブル制御部 3 6 と、出力ログ管理部 3 7 とで構成される。

【 0 1 4 8 】

なお、これらの各構成要素はそれぞれ専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。

【 0 1 4 9 】

また図中、太線で示す矢印は伝送容量の大きい伝送路を表しており、細線で示す矢印は伝送容量の比較的小さい伝送路を表している。もっとも現時点で想定されるシステム構成であり、伝送容量が大きい小さいかは相対的なものである。また現時点では細線の矢印で示す合わせ鍵の配信経路も伝送容量の大きいものとしてもよい。

【 0 1 5 0 】

(2 - 1 - 2) 各機能部の構成

まず、上流側システムを構成する各機能部を説明する。コンテンツサーバ 1 1 は、記録媒体（図 4 では磁気テープ）や伝送路を通じて提供を受けたデジタルコンテンツの蓄積を主な機能とする装置である。このため大容量のストレージ装置を備える。なお当該サーバはコンピュータ構成を採る。

【 0 1 5 1 】

すなわち、当該サーバは、制御機能と演算機能を実現する処理装置と、信号処理の実行に必要なデータを記憶する記憶装置と、外部からデータやプログラム及びコマンドを入力する入力装置と、処理結果を外部に出力する出力装置とを備える構成を採る。

【 0 1 5 2 】

コンテンツ符号化部 1 2 は、デジタルコンテンツの圧縮符号化その他の符号化処理を主な機能とする装置である。例えば、M P E G 変換や W a v e l e t 変換その他の符号化処理が実行される。なお、符号化処理は一般に 1 種類だけが行われるのではなく、運用時に広く採用されている複数の符号化処理が行われる。この結果、1 つのデジタルコンテンツに対して複数の符号化処理データが生成される。なお音声や画像データに透かし情報を埋め込む処理は、例えばコンテンツサーバ 1 1 とコンテンツ符号化部 1 2 との間で実行される。このコンテンツ符号化部 1 2 は、専用のハードウェアを用いて構成してもよいし、当該ハードウェアと同等の機能を実現させるプログラムがインストールされているコンピュータのソフトウェア上の処置として実現してもよい。

【 0 1 5 3 】

暗号化部 1 3 は、鍵発生部 1 6 からコンテンツに固有の暗号鍵の提供を受け、当該暗号鍵を用いてコンテンツ符号化処理の終了したデジタルコンテンツに暗号処理を施す装置である。ここで使用する暗号方式は運用時に広く採用されているものを用いればよい。

【 0 1 5 4 】

例えば、DES (Data Encryption Standard)、FEAL (Fast Data Encipherment Algorithm) その他の暗号処理が実行される。ここでの暗号処理は、業務データとコンテンツデータのそれぞれについて個別に実行される。参考までに言及すると、コンテンツデータについての暗号処理は、コンテンツ符号化部 1 2 で生成された各符号化データ毎に実行される。

【 0 1 5 5 】

なお暗号化部 1 3 も、専用のハードウェアを用いて構成してもよいし、コンピュータに同等の機能を実現させるソフトウェアの処理機能として実現してもよい。

【 0 1 5 6 】

送出サーバ 1 4 は、特定者のみが視聴又は記録できるように暗号化処理の施された（条件付きアクセス処理が施された）デジタルコンテンツをストレージ装置に蓄積する機能と、配信スケジュールに従って高速配信用ネットワーク 3 に出力する機能とを実現する装置である。ここでの出力機能は、広帯域伝送機能やレートコントロール機能を備える送信装置で実現される。

【 0 1 5 7 】

高速配信用ネットワーク 3 を用いたデータの配信は現在のところ夜間を利用した蓄積型の配信を想定しているが、伝送速度の向上が期待される将来においてはストリーミング配信等も想定する。

【 0 1 5 8 】

なお、デジタルコンテンツの配信を記録媒体の形態で実行する場合、前述した出力機能はデジタルコンテンツを所定の記録媒体に格納する記録装置で実現される。

【 0 1 5 9 】

コンテンツ管理サーバ 15 は、コンテンツサーバ 11 と通信し、新たに受付けたコンテンツの登録処理やコンテンツの検索処理、ファイル分割処理その他を実行する装置である。当該サーバもコンピュータ構成を採る。当該サーバではコンテンツ毎に発生された暗号鍵情報が管理される。例えば、コンテンツと対応する暗号鍵との関係がデータベースとして管理される。

【0160】

鍵発生部 16 は、配信対象であるデジタルコンテンツ毎に固有の暗号鍵を生成する手段である。暗号鍵の発生に使用される暗号方式は運用時に広く採用されているものを使用する。すなわち、不正な解読が困難な最新の暗号化技術に従う。

【0161】

配信先管理サーバ 17 は、コンテンツ毎に配信先と配信条件その他の業務データや配信先毎に生成した暗号鍵の情報をデータベースにより管理する装置である。ここでの配信条件には使用可能期間、出力可能回数その他の情報が含まれる。また当該サーバもコンピュータ構成を採る。

【0162】

図4に示すように、配信先管理サーバ 17 は、コンテンツ制作者 1 のシステムにのみ設ける場合、電子配信事業者 2 のシステムにのみ設ける場合、両者のシステム内に設ける場合が考えられる。これは各配信先に固有の鍵情報を誰が配信するかはビジネス上の選択事項だからである。ただし、鍵情報を知り得る事業者は少ないほどシステム全体からみた秘匿性は高まるため、コンテンツ制作者 1 のシステム内に配置するのが望ましい。

【0163】

合わせ鍵生成部 18 は、コンテンツ毎に生成された暗号鍵 A を配信先毎に固有の分割パターンで分割し、一組の合わせ鍵 A 1 及び A 2 を生成する装置である。例えば、配信先となる特定者が 1000 人いれば、1000 組の合わせ鍵 A 1 及び A 2 が生成される。生成された合わせ鍵は、合わせ鍵生成部 18 によって配信先管理サーバ 17 と所定の配信処理部に与えられる。このシステムの場合、合わせ鍵生成部 18 は、合わせ鍵 A 1 をネットワークを介した配信用に不図示の通信

部に与え、残る合わせ鍵 A 2 を記録媒体を介した配信用に書込部 1 9 に与える。

【 0 1 6 4 】

書込部 1 9 は、通知を受けた合わせ鍵 A 2 を所定の記録媒体に書き込むための装置である。書込部 1 9 には、記録媒体に応じた駆動機構が設けられる。記録媒体には、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他の媒体が用いられる。なお、記録媒体の配信に必要な宛先情報は配信先管理サーバ 1 7 から与えられる。前述の不図示の通信部についても同様である。ただし、通信部の場合にはネットワーク上のアドレスが与えられる。

【 0 1 6 5 】

次に、下流側システムを構成する各機能部を説明する。受信サーバ 3 1 は、特定者のみが視聴又は記録できるように暗号化処理の施された（条件付きアクセス処理が施された）デジタルコンテンツの受信機能と、配信を受けたデジタルコンテンツをストレージ装置に蓄積する機能と、再生スケジュールに従って復号サーバ 3 3 に出力する機能とを実現する装置である。ここでの受信機能は、受信データに含まれる誤り訂正等を行う機能も備える。

【 0 1 6 6 】

なお、デジタルコンテンツの配信を記録媒体の形態で受ける場合、前述した受信機能はデジタルコンテンツを所定の記録媒体から読み取る読取装置で実現される。

【 0 1 6 7 】

読取部 3 2 は、記録媒体の形態で配信される合わせ鍵 A 2 を記録媒体から読み取るための装置である。ここで駆動機構には、記録媒体に応じたものが用いられる。また、図中では表していないが、広域ネットワークを介して配信を受ける合わせ鍵 A 1 の受信用に通信部が設けられている。

【 0 1 6 8 】

復号サーバ 3 3 は、デジタルコンテンツに施されている暗号処理を解除する処理と、暗号が解除されたデジタルコンテンツに施されている符号化処理を復号化する処理とを実行する一方で、復元された生のデジタルコンテンツがそのまま装置外部に出力されないように局所的なスクランブル処理を施す装置である

【 0 1 6 9 】

復号サーバ 3 3 は、専用のハードウェアを用いて構成してもよいし、コンピュータに同等の機能を実現させるソフトウェアの処理機能として実現してもよい。因みに当該復号サーバ 3 3 は、悪意の特定者による不正行為からデジタルコンテンツを保護するため、正規の手続き以外ではその筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。これらの仕組みについては既存の技術を使用する。

【 0 1 7 0 】

特に、復号機能部 3 5（復号化部 3 5 A、鍵復元部 3 5 B、コンテンツ復号化部 3 5 C、スクランブル部 3 5 D）については、各機能ブロック間において重要な情報（暗号鍵や生のデジタルコンテンツ）が流れるため、不正行為を排除するための対策が重要であり、当該機能ブロック部分を半導体集積回路化したり、正規な手続き以外ではその筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。

【 0 1 7 1 】

ここで、復号化部 3 5 A は、鍵復元部 3 5 B から与えられる暗号鍵を用い、受信サーバ 3 1 から読み出されたデジタルコンテンツに施されている暗号処理（条件付きアクセス処理）を解除する機能部である。当該機能は専用のハードウェアで実現することもできるし、ソフトウェア上の機能として実現することもできる。

【 0 1 7 2 】

鍵復元部 3 5 B は、ネットワークを介して配信を受けた合わせ鍵 A 1 と記録媒体の形態で配信を受けた合わせ鍵 A 2 に基づいて、デジタルコンテンツに施されている暗号処理を解除できる暗号鍵を復元する機能を実現する機能部である。復元された暗号鍵は鍵復元部 3 5 B の管理下において所定の期間保持される。当該確認には不揮発性メモリ、ハードディスクその他の記録媒体が用いられる。

【 0 1 7 3 】

また鍵復元部 3 5 B は、受信サーバ 3 1 から読み出されたデジタルコンテン

ツの暗号を復号するのに先だって、当該デジタルコンテンツに付属されている業務データを読み出し、当該業務データで定められている再生条件が各時点において満たされているか否かの判定も行う。

【 0 1 7 4 】

ここで、鍵復元部 3 5 B は、再生条件が満たされるとき、復号化部 3 5 A に暗号解除許可信号を与える一方、スクランブル制御部 3 6 にスクランブル鍵の発生信号又は出力許可信号を与える。これに対し、鍵復元部 3 5 B は、再生条件が満たされないとき、復号化部 3 5 A に暗号解除禁止信号を与えると共に、スクランブル制御部 3 6 にスクランブル鍵の発生禁止信号又は出力禁止信号を与える。

【 0 1 7 5 】

コンテンツ復号化部 3 5 C は、特定者毎が採用しているコーデック方式に対応するものが用いられる。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。コンテンツ復号化部 3 5 C の信号処理の結果、暗号化処理前の生のデジタルコンテンツが復元される。

【 0 1 7 6 】

スクランブル部 3 5 D は、コンテンツ復号化部 3 5 C によって復元されたデジタルコンテンツがそのままの形態で出力されることがないように、スクランブル処理を施すための装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。

【 0 1 7 7 】

なお図 4 の場合、必要最小限の機能という意味でスクランブル制御部 3 6 を復号機能部 3 5 の外部にしているが、スクランブル制御部 3 6 を復号機能部 3 5 内の一機能として設けることも可能である。

【 0 1 7 8 】

スクランブル制御部 3 6 は、鍵復元部 3 5 B によりスクランブル鍵の発生が許可された場合、スクランブル鍵とこれと対をなすデスクランブル鍵を発生する。

【 0 1 7 9 】

なお、スクランブル鍵とデスクランブル鍵の発生方法には、コンテンツの違い

によらずいつも同じスクランブル鍵等を発生する方法（固定的に記憶されているスクランブル鍵とデスクランブル鍵を出力する方法）と、コンテンツ毎に異なるスクランブル鍵等を発生する方法（新たなコンテンツの出力のたび生成され、所定の再生条件が満たされる間保持される方法）と、再生出力のたびに異なるスクランブル鍵等を生成する方法（コンテンツの暗号を解除するたびに異なるスクランブル鍵を生成する方法）とがある。不正行為に対する防御機能の観点からは、記載順に 3 番目の方法、2 番目の方法、1 番目の方法の順番で不正が困難になる。

【0180】

出力ログ管理部 37 は、出力装置 34 からの不正出力を監視するため、出力装置 34 における出力ログを管理する装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。出力ログ管理部 37 は、出力ログを通信回線を通じて上流側システムを構成する配信先管理サーバ 17 に通知する。この結果、上流側システムでも別途、各特定者の再生出力状況を監視できる。また不正行為の発見にも利用できる。

【0181】

最後に、出力装置 34 の構成を説明する。出力装置 34 は、デジタルコンテンツに応じたものが用いられる。画像系であれば表示装置や投影装置が考えられるし、音声系であればスピーカが考えられる。いずれにしても、出力装置 34 は、その本来の機能部の他にデスクランブル部 34A を備える。

【0182】

デスクランブル部 34A は、復号サーバ 33 から与えられるデジタルコンテンツに施されているスクランブル処理を解除するための機能装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。当該デスクランブル部 34A は、半導体集積回路やボード部材で構成される。

【0183】

この出力装置 34 の場合も、デスクランブル部 34A から出力される信号につ

いては、電子透かしのような静的な保護機能しか施されていないため、正規の手続き以外では出力装置の筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。

【0184】

(2-1-3) デジタルコンテンツの配信動作

第1のシステムにおけるデジタルコンテンツの配信動作を簡単に説明する。当該システムでは、新たなデジタルコンテンツがコンテンツサーバ11に登録されると、コンテンツ管理サーバ15の管理下において当該コンテンツに固有の暗号鍵が発生される。次に、作成された暗号鍵が合わせ鍵生成部18に与えられ、各配信者に固有の分割パターンによって固有の合わせ鍵が生成される。

【0185】

ここで、各配信者に固有の分割パターンはコンテンツの違いにかかわらず同じものでもよいし、コンテンツ毎に異なる分割パターンを採用してもよい。いずれにしても、特定者毎にコンテンツに固有の合わせ鍵が生成される。

【0186】

その後、生成された合わせ鍵A1とA2がデジタルコンテンツの送信に先立って事前に配信される。このシステムの場合、合わせ鍵A1はネットワークを通じて、合わせ鍵A2は記録媒体に記録された形態で配信される。もっとも、常にデジタルコンテンツの配信に先立って行われなければならない訳ではない。暗号処理の解除に必要な鍵がデジタルコンテンツの配信後に行われる場合もあり得る。

【0187】

デジタルコンテンツと合わせ鍵の配信を受けた下流側システムが、所定の出力スケジュールに従ってデジタルコンテンツを読み出し、復元された暗号鍵で暗号処理を解除する。その後、暗号処理の解除されたデジタルコンテンツのうち特定者のシステム構成に適合するコーデック方式にかかるものが選択的に復号化され、復号結果についてのスクランブル処理が復号サーバ33にて実行される。

【0188】

この後、復号サーバ 3 3 からはスクランブル処理が施されたデジタルコンテンツが出力装置 3 4 に出力される。出力装置 3 4 では、スクランブル制御部 3 6 から与えられるデスクランブル鍵によってスクランブル処理の解除が行われ、所望の形態でコンテンツの出力が行われる。

【 0 1 8 9 】

(2 - 1 - 4) 第 1 のシステムによって得られる効果

上述のように第 1 のシステムによれば、合わせ鍵の配信経路を複数としたことにより、たとえいずれかの合わせ鍵が盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、合わせ鍵をデジタルコンテンツとは別の経路（上述のように同一の経路を用いながら時間的に別の時点に配信する場合を含む。）で配信する場合には、合わせ鍵の一部を盗んだ不正行為者が暗号化されたデジタルコンテンツをも入手した場合でも、暗号鍵の復元に必要な鍵情報はデジタルコンテンツとは別に配信されるため、生のデジタルコンテンツが復号化される事態を確実に回避できる。

【 0 1 9 0 】

また、暗号処理が解除されたデジタルコンテンツにスクランブル処理を施す方式を採用したことにより、不正行為に対する十分な防御能力を保持したままで復号機能を実行するサーバ装置と再生機能を実行する出力装置との分離を実現できる。

【 0 1 9 1 】

特に、運用後により安全性が高い暗号方式が出現した場合や取り扱うコーデック方式を変更したい場合でも、復号サーバ 3 3 のみを置き換えることで対処できる。また、特定者が取り扱うコーデック方式が何であったとしても、復号サーバ 3 3 から出力装置 3 4 に出力されるデータはスクランブル処理されたデータに統一されるため、出力装置 3 4 を複数のコーデック方式で共用できる。

【 0 1 9 2 】

このことは出力装置 3 4 の開発費が少なく済むことをも意味する。すなわち、汎用型の出力装置 3 4 にデスクランブル部 3 4 A を搭載すると共に、正規な手続きでしか開封できないか又は動作しない仕組みを搭載するだけでよいため、出力

装置 3 4 の低価格化を実現できる。従って、運用後により性能の高い出力装置が開発された場合でも、例えば再現解像度の高いものが開発された場合でも、装置の置き換えが進み易い。

【 0 1 9 3 】

かくして、不正行為に対する安全性もシステムを運用する上での経済性も同時に満足できる。

【 0 1 9 4 】

(2 - 2) 第 2 のシステム例

(2 - 2 - 1) システム構成

図 5 に、上述のビジネスモデルを実現するための第 2 のシステム例を示す。ここで図 5 は、図 4 との対応部分に同一符号を付して表したものである。図 5 と図 4 を対比して分かるように、当該システムを構成する下流側システムは第 1 のシステム例と同じである。

【 0 1 9 5 】

本システムと第 1 のシステム例との違いは、合わせ鍵生成部 1 8 で生成された合わせ鍵 A 1 を更に分割する部分鍵生成部 2 0 が追加された点と、当該部分鍵生成部 2 0 で生成された部分鍵を記録媒体に書き込むための書込部 2 1 とその読み取り用の読取部 3 8 が設けられた点と、配信される鍵情報が 3 つになったことに伴って鍵情報の配信方法に一部変更が生じた点である。

【 0 1 9 6 】

部分鍵生成部 2 0 は、合わせ鍵生成部 1 8 の分割処理により得られた合わせ鍵の一部 A 1 を所定の分割パターンで分割し、一組の部分鍵 A 1 1 及び A 1 2 を生成する装置である。例えば、配信先となる特定者が 1 0 0 0 人いれば、1 0 0 0 組の部分鍵 A 1 1 及び A 1 2 が生成される。なお所定の分割パターンは配信先毎に異なってもよいし、同じでもよい。

【 0 1 9 7 】

生成された部分鍵は、部分鍵生成部 2 0 によって配信先管理サーバ 1 7 と所定の配信処理部とに与えられる。このシステムの場合、部分鍵生成部 2 0 は、部分鍵 A 1 1 をネットワークを介しての配信用に不図示の通信部とに与え、残る部分鍵 A

1 2 を記録媒体による配信用に書込部 2 1 に与える。

【0 1 9 8】

書込部 2 1 は、通知を受けた部分鍵 A 1 2 を所定の記録媒体に書き込むための装置である。書込部 2 1 には、記録媒体に応じた駆動機構が設けられる。記録媒体には、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他の媒体が用いられる。なお、記録媒体の配信に必要な宛先情報は配信先管理サーバ 1 7 から与えられる。前述の不図示の通信部についても同様である。ただし、通信部の場合にはネットワーク上のアドレスが与えられる。

【0 1 9 9】

なお当該書込部 2 1 と対をなす読取部 3 8 には、配信を受ける記録媒体に応じた駆動機構を備えるものが用いられる。

【0 2 0 0】

また、第 1 のシステム例では、合わせ鍵生成部 1 8 で生成された合わせ鍵 A 2 は記録媒体を通じて下流側システムに配信されていたが、この第 2 のシステム例の場合、合わせ鍵 A 2 はネットワークを介して配信される。

【0 2 0 1】

以上が第 2 のシステム例と第 1 のシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、デジタルコンテンツの配信動作は部分鍵の発生以外同様に実行される。

【0 2 0 2】

(2 - 2 - 2) 第 2 のシステムによって得られる効果

以上のように第 2 のシステムによれば、鍵情報の配信を 2 つの伝送網（異なる伝送網を用いる場合と、同一伝送網に異なる時点で鍵情報を配信する場合とがある。）と記録媒体とで実現するため、すなわち第 1 のシステムよりも更に鍵情報の配信経路が増えるため、伝送経路上での不正行為がより困難なものを提供できる。

【0 2 0 3】

(2 - 3) 第 3 のシステム例

(2 - 3 - 1) システム構成

図 6 に、上述のビジネスモデルを実現するための第 3 のシステム例を示す。ここで図 6 は、図 4 及び図 5 との対応部分に同一符号を付して表したものである。

【 0 2 0 4 】

本システムにおける上流側システムと第 2 のシステム例との違いは、合わせ鍵 A 2 の配信がネットワークを介して行われるのではなく、第 1 のシステム例のように記録媒体を通じて実現される点である。このため、合わせ鍵 A 2 の配信経路については、第 1 のシステム例と同じものが用いられている。

【 0 2 0 5 】

以上が第 3 のシステムと上述したシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、デジタルコンテンツの配信動作は第 1 のシステムや第 2 のシステムと同様である。

【 0 2 0 6 】

(2 - 3 - 2) 第 3 のシステムによって得られる効果

以上のように第 3 のシステムによれば、鍵情報の配信を 1 つの伝送網と 2 つの記録媒体とで実現するため、すなわち第 2 のシステムよりも記録媒体による配信経路が増えるため、鍵情報の盗難を発見し易いより不正行為に対する安全性の高いものを提供できる。

【 0 2 0 7 】

(2 - 4) 第 4 のシステム例

(2 - 4 - 1) システム構成

図 7 に、上述のビジネスモデルを実現するための第 4 のシステム例を示す。ここで図 7 は、図 4 との対応部分に同一符号を付して表したものである。

【 0 2 0 8 】

本システムにおける上流側システムと第 1 のシステム例との違いは、合わせ鍵生成部 1 8 で発生された合わせ鍵 A 1 及び A 2 がいずれもネットワークを介して配信される点である。

【 0 2 0 9 】

以上が第 4 のシステムと第 1 のシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、デジタルコンテンツの配信動作は

第 1 のシステムと同様である。

【 0 2 1 0 】

(2 - 4 - 2) 第 4 のシステムによって得られる効果

以上のように第 4 のシステムによれば、鍵情報の配信を 2 つともネットワークを介して実現するため、すなわち全ての鍵情報を即時性に優れたネットワークを通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からデジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。

【 0 2 1 1 】

(2 - 5) 第 5 のシステム例

(2 - 5 - 1) システム構成

図 8 に、上述のビジネスモデルを実現するための第 5 のシステム例を示す。ここで図 8 は、図 4 との対応部分に同一符号を付して表したものである。

【 0 2 1 2 】

本システムにおける上流側システムと第 1 のシステム例との違いは、合わせ鍵生成部 1 8 で発生された合わせ鍵 A 1 及び A 2 がいずれも記録媒体を介して配信される点である。このため、本システムでは、合わせ鍵 A 1 を記録媒体に書き込むための書込部 2 2 と、これと対をなす読取部 3 9 とが新たに設けられている。書込部 2 2 や読取部 3 9 の構成は、他の書込部や読取部の構成と同じである。

【 0 2 1 3 】

以上が第 5 のシステムと第 1 のシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、デジタルコンテンツの配信動作は第 1 のシステムと同様である。

【 0 2 1 4 】

(2 - 5 - 2) 第 5 のシステムによって得られる効果

以上のように第 5 のシステムによれば、鍵情報の配信を 2 つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【 0 2 1 5 】

(2 - 6) 第 6 のシステム例

(2 - 6 - 1) システム構成

図 9 に、上述のビジネスモデルを実現するための第 6 のシステム例を示す。ここで図 9 は、図 5 との対応部分に同一符号を付して表したものである。

【 0 2 1 6 】

本システムにおける上流側システムと第 2 のシステム例（図 5）との違いは、部分鍵生成部 2 0 で発生された部分鍵 A 1 2 がネットワークを介して配信される点である。

【 0 2 1 7 】

以上が第 6 のシステムと第 2 のシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、デジタルコンテンツの配信動作は第 2 のシステムと同様である。

【 0 2 1 8 】

(2 - 6 - 2) 第 6 のシステムによって得られる効果

以上のように第 6 のシステムによれば、鍵情報の配信を 3 つともネットワークを介して実現するため、すなわち全ての鍵情報を即時性に優れたネットワークを通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からデジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。

【 0 2 1 9 】

更に、配信される鍵情報の数が 3 つであるため、2 つの鍵情報をネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【 0 2 2 0 】

(2 - 7) 第 7 のシステム例

(2 - 7 - 1) システム構成

図 1 0 に、上述のビジネスモデルを実現するための第 7 のシステム例を示す。ここで図 1 0 は、図 6 及び図 8 との対応部分に同一符号を付して表したものである。

る。

【 0 2 2 1 】

本システムにおける上流側システムと第 3 のシステム例との違いは、部分鍵生成部 2 0 で発生された部分鍵 A 1 1 及び A 1 2 がいずれも記録媒体を介して配信される点である。このため、本システムでは、部分鍵 A 1 1 を記録媒体に書き込むための書込部 2 2 と、これと対をなす読取部 3 9 とが新たに設けられている。書込部 2 2 や読取部 3 9 の構成は、他の書込部や読取部の構成と同じである。

【 0 2 2 2 】

以上が第 7 のシステムと第 3 のシステム例との相違点である。なお基本的なシステム構成については何ら変更がないため、デジタルコンテンツの配信動作は第 3 のシステムと同様である。

【 0 2 2 3 】

(2 - 7 - 2) 第 7 のシステムによって得られる効果

以上のように第 7 のシステムによれば、鍵情報の配信を 3 つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する経路を含む場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【 0 2 2 4 】

(2 - 8) 第 8 のシステム例

(2 - 8 - 1) システム構成

図 1 1 に、上述のビジネスモデルを実現するための第 8 のシステム例を示す。ここで図 1 1 は、図 4 との対応部分に同一符号を付して表したものである。当該システムは、前述までの第 1 ～第 7 のシステムとは異なり、デジタルコンテンツの暗号鍵を分割するのではなく、当該暗号鍵を配信先に固有の別の多重鍵で暗号化する。

【 0 2 2 5 】

このため、第 8 のシステムでは、配信先に固有の多重鍵 B を生成する多重鍵生成部 2 3 と、当該多重鍵 B によって暗号鍵 A を暗号化する鍵暗号化処理部 2 4 と、多重鍵 B を記録媒体に書き込んで配信するのに使用する書込部 2 5 と、これと

対をなす読取部 4 0 を、第 1 のシステムにおける合わせ鍵生成部 1 8、書込部 1 9、読取部 3 2 に置き換えて使用する。

【 0 2 2 6 】

多重鍵生成部 2 3 は、コンテンツ毎に生成された暗号鍵 A に配信先毎に固有の暗号鍵 B を生成する装置である。例えば、配信先となる特定者が 1 0 0 0 人いれば、1 0 0 0 通りの多重鍵 B を生成する。もっとも多重鍵 B は、配信先が同じであれば常に同じ多重鍵を用いる方法もあれば、コンテンツ毎に異なる多重鍵 B を生成して用いる場合もある。安全性の観点からは後者が望ましい。

【 0 2 2 7 】

鍵暗号化処理部 2 4 は、配信先毎に固有の多重鍵を用いて暗号鍵を暗号化する装置である。鍵暗号化処理部 2 4 で暗号化された暗号鍵は、不図示の通信部よりネットワークを介して対応する下流側システムに配信される。

【 0 2 2 8 】

書込部 2 5 と読取部 4 0 の構成は上述の書込部及び読取部と同じである。もっとも、書込部 2 5 と読取部 4 0 によって読み書きされるのは多重鍵である点で上述のシステムとは異なる。

【 0 2 2 9 】

(2 - 8 - 2) デジタルコンテンツの配信動作

第 8 のシステムにおけるデジタルコンテンツの配信動作のうち第 1 のシステムと異なる部分についてのみ簡単に説明する。すなわち、第 1 のシステムでは、コンテンツに固有の暗号鍵 A を発生すると当該暗号鍵を合わせ鍵生成部 1 8 に与えて合わせ鍵を生成したが、本システムの場合、配信先毎に発生された固有の多重鍵 B を用いて暗号鍵 A を暗号化し、ネットワークを介して下流側システムに配信する。また、当該暗号鍵 A の暗号化に使用した多重鍵 B をそれぞれ対応するは威信者に宛てて記録媒体の形態で配信する。

【 0 2 3 0 】

なお生成された多重鍵 B は、配信先管理サーバ 1 7 にて管理される。以上の処理動作が第 1 のシステムとの主な違いである。

【 0 2 3 1 】

(2-8-3) 第8のシステムによって得られる効果

上述のように第8のシステムによれば、下流側システムを管理する特定者に配信する鍵情報を暗号化された暗号鍵Aと多重鍵Bとの2つとし、それらを複数の経路を介して配信する構成としたことにより、たとえいずれかの鍵情報が盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。

【0232】

しかも多重鍵については盗難を発見し易い記録媒体の形態で配信を行うため、不正行為によって多重鍵が盗難されたことが明らかになった場合にはネットワークを介して行う暗号化された暗号鍵Aの配信を行うのを中止し、別の多重鍵Bを記録媒体として配信する手順から再開することで不正行為に対する安全性を保つことができる。

【0233】

勿論、下流側システムの構成は第1のシステムと同じであるため、運用に際しての経済性にも優れることは第1のシステムと同様である。

【0234】

(2-9) 第9のシステム例

(2-9-1) システム構成

図12に、上述のビジネスモデルを実現するための第9のシステム例を示す。ここで図12は、図11との対応部分に同一符号を付して表したものである。

【0235】

本システムと第8のシステム例との違いは、多重鍵生成部23で生成された多重鍵Bを分割し、一組の合わせ鍵B1とB2を生成する合わせ鍵生成部26が追加された点と、当該合わせ鍵生成部26で生成された合わせ鍵の一部B2を記録媒体に書き込むための書込部27とその読み取り用の読取部41が設けられた点である。

【0236】

合わせ鍵生成部26は、配信先毎に生成された多重鍵Bを配信先毎に固有の分割パターンで分割し、一組の合わせ鍵B1及びB2を生成する装置である。合わ

せ鍵生成部 2 6 の分割規則は、全ての配信先について共通の分割規則を用いることも可能であるし、配信先毎に固有の分割規則を割り当てることも可能であるし、これら分割規則をコンテンツ単位で変更することも可能である。

【 0 2 3 7 】

書込部 2 7 と読取部 4 1 の構成は他の書込部や読取部と同じである。なお基本的なシステム構成については何ら変更がないため、デジタルコンテンツの配信動作は第 8 のシステムと同様である。

【 0 2 3 8 】

(2 - 9 - 2) 第 9 のシステムによって得られる効果

以上のように第 9 のシステムによれば、多重鍵 B を一組の合わせ鍵 B 1 及び B 2 に分割して一方をネットワークで、他方を記録媒体で配信する構成を採用するため、すなわち多重鍵 B そのものを送るのではなく分割したものを配信するのに加え、配信経路を 2 つから 3 つに増やすことにより、第 8 のシステムに比べてより不正行為に対する安全性の高いものを提供できる。

【 0 2 3 9 】

(2 - 1 0) 第 1 0 のシステム例

(2 - 1 0 - 1) システム構成

図 1 3 に、上述のビジネスモデルを実現するための第 1 0 のシステム例を示す。ここで図 1 3 は、図 1 2 との対応部分に同一符号を付して表したものである。

【 0 2 4 0 】

本システムと第 9 のシステム例との違いは、暗号化された暗号鍵 A の配信をネットワークを介して行うのではなく、記録媒体を介して行う点である。このため、本システムの場合には、書込部 2 8 と読取部 4 2 が新たに設けられる点で異なっている。書込部 2 8 と読取部 4 2 の構成は他の書込部や読取部と同じであるため省略する。

【 0 2 4 1 】

なお基本的なシステム構成については何ら変更がないため、デジタルコンテンツの配信動作は第 8 のシステムと同様である。

【 0 2 4 2 】

(2-10-2) 第10のシステムによって得られる効果

以上のように第10のシステムによれば、暗号化された暗号鍵Aが記録媒体を通じて配信される分、当該鍵がネットワークを介して配信される場合に比して盗難の早期発見が可能となり、暗号鍵の変更等の対策を採り易いという効果を期待できる。

【0243】

(2-11) 第11のシステム例

(2-11-1) システム構成

図14に、上述のビジネスモデルを実現するための第11のシステム例を示す。ここで図14は、図11との対応部分に同一符号を付して表したものである。

【0244】

本システムと第8のシステムとの違いは、多重鍵Bを記録媒体を介して行うのではなく、ネットワークを介して行う点である。それ以外は第8のシステムと同じであるため、デジタルコンテンツの配信動作は第8のシステムと同様である。もっとも、多重鍵Bの配信に際しては、デジタル証明書等で相手方の正当性を確認した上で、配信先が公開している公開鍵で暗号化して配信するのが望ましい。

【0245】

(2-11-2) 第11のシステムによって得られる効果

以上のように第11のシステムによれば、多重鍵Bをネットワークを介して配信する手法を採用するため、鍵の配信からデジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。

【0246】

(2-12) 第12のシステム例

(2-12-1) システム構成

図15に、上述のビジネスモデルを実現するための第12のシステム例を示す。ここで図15は、図11及び図13との対応部分に同一符号を付して表したものである。

【0247】

本システムと第 8 のシステム例との違いは、暗号化された暗号鍵 A の配信をネットワークを介して行うのではなく、記録媒体を介して行う点である。それ以外は第 8 のシステムと同じであるため、デジタルコンテンツの配信動作は第 8 のシステムと同様である。

【 0 2 4 8 】

(2 - 1 2 - 2) 第 1 2 のシステムによって得られる効果

以上のように第 1 2 のシステムによれば、鍵情報の配信を 2 つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【 0 2 4 9 】

(2 - 1 3) 第 1 3 のシステム例

(2 - 1 3 - 1) システム構成

図 1 6 に、上述のビジネスモデルを実現するための第 1 3 のシステム例を示す。ここで図 1 6 は、図 1 2 との対応部分に同一符号を付して表したものである。

【 0 2 5 0 】

本システムと第 9 のシステムとの違いは、多重鍵 B から生成した合わせ鍵 B 2 の配信に記録媒体を用いるのではなく、ネットワークを介して行う点である。すなわち、3 つの鍵情報の配信を全てネットワークを介して行う点で異なっている。それ以外は第 9 のシステムと同じであるため、デジタルコンテンツの配信動作は第 9 のシステムと同様である。

【 0 2 5 1 】

(2 - 1 3 - 2) 第 1 3 のシステムによって得られる効果

以上のように第 1 3 のシステムによれば、鍵情報の配信を 3 つともネットワークを介して行うため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からデジタルコンテンツの配信が開始されるまでの時間を大幅に短縮できる。

【 0 2 5 2 】

更に、配信される鍵情報の数が 3 つであるため、2 つの鍵情報をネットワーク

を介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【0253】

(2-14) 第14のシステム例

(2-14-1) システム構成

図17に、上述のビジネスモデルを実現するための第14のシステム例を示す。ここで図17は、図13との対応部分に同一符号を付して表したものである。

【0254】

本システムと第10のシステムとの違いは、多重鍵Bから生成した合わせ鍵B1の配信にネットワークを用いるのではなく、記録媒体を介して行う点である。すなわち、3つの鍵情報の配信を全て記録媒体を介して行う点で異なっている。このため、本システムの場合には、書込部29と読取部43が新たに設けられている。書込部29と読取部43の構成は他の書込部や読取部と同じであるため省略する。

【0255】

それ以外は第10のシステムと同じであるため、デジタルコンテンツの配信動作は第10のシステムと同様である。

【0256】

(2-14-2) 第14のシステムによって得られる効果

以上のように第14のシステムによれば、鍵情報の配信を3つとも記録媒体を介して行うため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する経路を含む場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【0257】

(3) 各システム例で想定される運用形態

第1～第14のシステム例では、上流側システムを構成する機能部のいずれがコンテンツ制作会社1のシステム内で行われ、いずれが電子配信事業者2のシステム内で行われるか問題とすることなく、当該システム構成から認められる技術的な効果の観点から説明を行ったが、ここでは想定される運用形態についてビジ

ネス上の効果にどのような差異が生じるかについて説明する。特に、コンテンツ制作会社 1 の立場からみた得失について説明する。

【 0 2 5 8 】

図 1 8 は、上流側システムを構成する機能部のうち、コンテンツ符号化部 1 2 と、暗号化部 1 3 と、鍵発生部 1 6（間接的には合わせ鍵生成部（部分鍵生成部）や多重鍵生成部（その合わせ鍵生成部））がどのように配置されるかの観点からまとめたものである。ただし、図 1 8 では、配信される鍵情報が 2 種類の場合について示されている。3 種類以上の鍵情報が配信される場合には、図 1 8 に「1 つ」と表記された箇所は、「少なくとも 1 つ」を意味する。

【 0 2 5 9 】

（ 3 - 1 ） 第 1 の運用形態

第 1 の運用形態では、暗号鍵 A の発生者、符号化処理の実行者、暗号処理の実行者のいずれもがコンテンツ制作会社である場合（すなわち、コンテンツ符号化部 1 2、暗号化部 1 3、鍵発生部 1 6 がコンテンツ制作会社のシステム側に設けられる場合）であって、鍵情報の配信もコンテンツ制作会社が行う場合を考える。

【 0 2 6 0 】

ここで、鍵情報の発生は配信主体であるコンテンツ制作会社が行う場合を想定する。すなわち、合わせ鍵生成部 1 8（システム例によっては部分鍵生成部 2 0 も含む。）や多重鍵生成部 2 3 及び鍵暗号化処理部 2 4（システム例によっては合わせ鍵生成部 2 6 も含む。）もコンテンツ制作会社が行う場合を想定する。

【 0 2 6 1 】

この場合、電子配信事業者 2 のシステムは暗号処理の施されたデジタルコンテンツを特定者に配信するだけの業務を行うことになる。すなわち、送出サーバ 1 4 のみが電子配信事業者 2 のシステムに属することになる。

【 0 2 6 2 】

このような運用形態を採ると、デジタルコンテンツの暗号化に使用した暗号鍵（マスター鍵）を知り得る立場にある者はコンテンツ制作会社 1 のみとできる。このことは、コンテンツ制作会社 1 からみると、電子配信事業者 2 を通じて暗

号鍵が外部に流出する危険性を一切考慮しなくて済むため、安心してコンテンツの提供を行えるという利点がある。ただし、多くの信号処理を自前で行う必要があるため、設備投資を行う経済的余力のないコンテンツ作会社にとっては選択が難しい運用態様である。

【 0 2 6 3 】

(3 - 2) 第 2 の運用形態

第 2 の運用形態では、基本的には第 1 の運用形態の下に、鍵情報の配信主体がコンテンツ制作会社 1 と電子配信事業者 2 の 2 者となる場合を考える。

【 0 2 6 4 】

例えば、第 2 のシステム例（図 5）において合わせ鍵 A 2 の生成と配信はコンテンツ制作会社 1 が行うが、合わせ鍵 A 1 から部分鍵 A 1 1 と A 1 2 を生成する処理と生成された部分鍵の配信は電子配信事業者 2 が行う場合が考えられる。この他同様の場合に、第 3 のシステム例（図 6）、第 6 のシステム例（図 9）、第 7 のシステム例（図 1 0）が考えられる。

【 0 2 6 5 】

また例えば、生成された合わせ鍵や部分鍵の記録媒体への書込みと配信のみを電子配信事業者 2 に実行させる場合も考えられる。かかる場合には、第 1 のシステム例（図 4）、第 2 のシステム例（図 5）、第 3 のシステム例（図 6 において部分鍵 A 1 2 及び又は合わせ鍵 A 2 を書き込む場合）、第 5 のシステム例（図 8 で合わせ鍵 A 1 又は A 2 を書き込む場合）、第 7 のシステム例（図 1 0 でいずれか 1 つの鍵情報又はいずれか 2 つの鍵情報を書き込む場合）、第 9 のシステム例（図 1 2 で合わせ鍵 B 2 を書き込む場合）、第 1 0 のシステム例（図 1 3 で暗号化された暗号鍵又は合わせ鍵 B 2 を書き込む場合）、第 1 2 のシステム例（図 1 5 で暗号化された暗号鍵を書き込む場合）、第 1 4 のシステム例（図 1 7 でいずれか 1 つの鍵情報又はいずれか 2 つの鍵情報を書き込む場合）がある。

【 0 2 6 6 】

このような運用形態としても、デジタルコンテンツの暗号化に使用した暗号鍵（マスター鍵）を知り得る立場にある者はコンテンツ制作者のみとなるため、コンテンツ制作会社 1 にとって安全な運用形態とできる。

【 0 2 6 7 】

なお以上のものに比べるとやや信頼性は低下するが同様の効果が期待できるものに、第 9 のシステム例（図 1 2）において暗号鍵 A の暗号化と配信はコンテンツ制作会社 1 が行うが、多重鍵 B の合わせ鍵 B 1、B 2 の生成と生成された合わせ鍵の配信は電子配信事業者 2 が行う場合が考えられる。

【 0 2 6 8 】

これと同様のものに第 1 0 のシステム例（図 1 3）、第 1 2 のシステム例（図 1 5）、第 1 3 のシステム例（図 1 6）、第 1 4 のシステム例（図 1 7）が考えられる。

【 0 2 6 9 】

（ 3 - 3 ） 第 3 の運用形態

第 3 の運用形態では、基本的には第 1 の運用形態の下に、鍵情報の配信主体が電子配信事業者 2 となる場合を考える。

【 0 2 7 0 】

例えば、第 1 のシステム例（図 4）において、暗号鍵の発生はコンテンツ制作会社 1 が行うが、発生された暗号鍵を入手して合わせ鍵 A 1、A 2 を生成する処理は電子配信事業者 2 が行う場合が考えられる。これはいずれのシステム例の場合にも考えられる。

【 0 2 7 1 】

かかる運用形態を採ると、デジタルコンテンツの暗号化に使用した暗号鍵（マスター鍵）を知り得る立場にある者がコンテンツ制作会社 1 と電子配信事業者 2 の 2 者となるため、第 1 の運用形態や第 2 の運用形態よりは暗号鍵が外部に流出する危険性が増えることになる。このため図 1 8 では安全性を中程度としている。

【 0 2 7 2 】

（ 3 - 4 ） 第 4 ～ 第 6 の運用形態

これらの運用形態では、第 1 ～ 第 3 の運用形態と異なり、暗号化処理を電子配信事業者 2 が実行する場合を考える。すなわち、電子配信事業者 2 が暗号鍵をコンテンツ制作会社 1 から入手して暗号処理を実行する場合である。なお、これら

の例では符号化処理はコンテンツ制作会社 1 側が実行するものとする。

【0 2 7 3】

これらの場合では、鍵情報の配信主体がコンテンツ制作会社 1 のみであるか、電子配信事業者 2 のみであるか、その両者であるかによらず、結局のところ暗号鍵を知り得る立場にある者がコンテンツ制作会社 1 と電子配信事業者 2 の 2 者となる。従って、コンテンツ制作会社の側からみた安全性は中程度となる。

【0 2 7 4】

(3-5) 第 7～第 9 の運用形態

これらの運用形態では、第 4～第 6 の運用形態に更に加えて、符号化処理の実行も電子配信事業者 2 が行う場合を考える。これらの運用形態では、コンテンツ制作会社 1 はもはや暗号鍵を生成しているだけにすぎず、鍵情報の配信主体がコンテンツ制作会社 1 のみであるか、電子配信事業者 2 のみであるか、その両者であるかによらず、結局のところ暗号鍵を知り得る立場にある者がコンテンツ制作会社 1 と電子配信事業者 2 の 2 者となる。従って、コンテンツ制作会社の側からみた安全性は中程度となる。

【0 2 7 5】

(3-6) 第 10～第 12 の運用形態

これらの運用形態では、暗号鍵の生成を電子配信事業者 2 が行って、デジタルコンテンツの暗号化は電子配信事業者 2 から暗号鍵の通知を受けたコンテンツ制作会社 1 が実施する場合を考える。この場合も、鍵情報の配信主体に誰になるかにかかわらず、結局のところ暗号鍵を知り得る立場にある者はコンテンツ制作会社 1 と電子配信事業者 2 の 2 者となる。ただし、コンテンツ制作会社 1 は、暗号鍵の管理上は受身にならざる得ないので、コンテンツ制作会社の側からみた安全性は小さくなる。

【0 2 7 6】

(3-7) 第 13～第 18 の運用形態

これらのうち第 13～第 15 の運用形態は、暗号鍵の生成と暗号化処理を電子配信事業者 2 が実施し、符号化処理のみをコンテンツ事業者が行う場合である。また第 16～第 18 の運用形態は、暗号鍵の生成、符号化処理、暗号化処理のい

ずれをも電子配信事業者 2 が行う場合である。

【 0 2 7 7 】

いずれの運用形態の場合も、鍵情報の配信主体に誰になるかにかかわらず、結局のところ暗号鍵を知り得る立場にある者はコンテンツ制作会社 1 と電子配信事業者 2 の 2 者となり、しかもコンテンツ制作会社 1 は、暗号鍵の管理上は受身にならざるを得ないので、コンテンツ制作会社の側からみた安全性は小さくなる。

【 0 2 7 8 】

【発明の効果】

(1) 請求項 1 ～ 1 5 のいずれかに記載の発明によれば、デジタルコンテンツを各コンテンツに固有の暗号鍵で暗号化して配信する仕組みを採用することにより、あるデジタルコンテンツに対する被害が他のデジタルコンテンツに及ばない配信方法を実現できる。また、各コンテンツに固有の暗号鍵を基に生成される各特定者に固有の合わせ鍵や部分鍵を複数の配信経路を用いて個別に配信するようにしたことにより、暗号鍵を復元するのに必要な全ての情報を一度に入手するのが困難な配信方法を実現できる。また、下流側システムを、暗号処理の解除されたデジタルコンテンツにスクランブル処理を施して出力する復号サーバと、当該スクランブル処理を解除する出力装置とで構成することにより、復号サーバと出力装置の伝送路上でも不正複製が困難な配信方法を実現できる。

【 0 2 7 9 】

(2) 請求項 1 6 に記載の発明によれば、下流側システムを、暗号処理の解除されたデジタルコンテンツにスクランブル処理を施して出力する復号サーバと、当該スクランブル処理を解除する出力装置とで構成することにより、復号サーバと出力装置の伝送路上でも不正複製が困難な下流側システムを実現できる。

【 0 2 8 0 】

(3) 請求項 1 7 に記載の発明によれば、その出力信号からはデジタルコンテンツの不正複製が困難な復号サーバを実現できる。また、請求項 1 8 に記載の発明によれば、当該回路装置を電子機器に搭載するだけで請求項 1 7 の復号サーバと同様の機能を実現できる。また、請求項 1 9 に記載の発明によれば、専用装置を用いなくても、請求項 1 7 の復号サーバと同様の機能を実現することができ

る。また、請求項 2 0 に記載の発明によれば、スクランブル制御部と別途組み合わせることで、請求項 1 7 の復号サーバと同様の機能を容易に実現可能な復号サーバを実現できる。同様に、請求項 2 1 に記載の発明によれば、当該回路装置とスクランブル制御部とを別途組み合わせて電子機器に搭載するだけで請求項 1 7 の復号サーバと同様の機能を実現できる。また、請求項 2 2 に記載の発明によれば、コンピュータをスクランブル制御部として機能させるプログラムと組み合わせることで、専用装置を用いなくても、請求項 1 7 の復号サーバと同様の機能を実現することができる。また、請求項 2 3 に記載の発明によれば、請求項 2 0 に記載の発明と組み合わせることで、請求項 1 7 の復号サーバと同様の機能を容易に実現可能な復号サーバを実現できる。同様に、請求項 2 4 に記載の発明によれば当該回路装置と請求項 2 1 に記載の回路装置とを別途組み合わせて電子機器に搭載するだけで請求項 1 7 の復号サーバと同様の機能を実現できる。また、請求項 2 5 に記載の発明によれば、請求項 2 2 に記載のプログラムと組み合わせることで、専用装置を用いなくても、請求項 1 7 の復号サーバと同様の機能を実現することができる。

【 0 2 8 1 】

(4) 請求項 2 6 に記載の発明によれば、その入力信号からはデジタルコンテンツの不正複製が困難な出力装置を実現できる。また、請求項 2 7 に記載の発明によれば、当該回路装置を電子機器に搭載するだけで請求項 2 6 の出力装置と同様の機能を実現できる。また、請求項 2 8 に記載の発明によれば、専用装置を用いなくても、請求項 2 6 の出力装置と同様の機能を実現することができる。

【 0 2 8 2 】

(5) 請求項 2 9 に記載の発明によれば、復号サーバが暗号処理の解除されたデジタルコンテンツにスクランブル処理を施して出力する仕組みを採用し、他方、出力装置がデジタルコンテンツに施されているスクランブル処理を解除して所定の出力形態で再生する仕組みを採用することにより、復号サーバと出力装置の伝送路上でも不正複製が困難な下流側システムにおける信号処理方法を実現できる。

【 0 2 8 3 】

(6) 請求項 30 に記載の発明によれば、復号サーバが暗号処理の解除されたデジタルコンテンツにスクランブル処理を施して出力する仕組みを採用することにより、その出力信号からはデジタルコンテンツの不正複製が困難な復号サーバにおける信号処理方法を実現できる。

【図面の簡単な説明】

【図 1】

本発明にかかる配信システムの概念を説明する概念構成図である。

【図 2】

本発明にかかる配信システムにおける高速配信用ネットワークで配信されるデータのデータ構造を示す図である。

【図 3】

本発明にかかる配信システムを映画コンテンツに適用した場合について示す図である。

【図 4】

本発明の実施の形態における第 1 の配信システムの構成例を示すブロック図である。

【図 5】

本発明の実施の形態における第 2 の配信システムの構成例を示すブロック図である。

【図 6】

本発明の実施の形態における第 3 の配信システムの構成例を示すブロック図である。

【図 7】

本発明の実施の形態における第 4 の配信システムの構成例を示すブロック図である。

【図 8】

本発明の実施の形態における第 5 の配信システムの構成例を示すブロック図である。

【図 9】

本発明の実施の形態における第 6 の配信システムの構成例を示すブロック図である。

【図 1 0】

本発明の実施の形態における第 7 の配信システムの構成例を示すブロック図である。

【図 1 1】

本発明の実施の形態における第 8 の配信システムの構成例を示すブロック図である。

【図 1 2】

本発明の実施の形態における第 9 の配信システムの構成例を示すブロック図である。

【図 1 3】

本発明の実施の形態における第 1 0 の配信システムの構成例を示すブロック図である。

【図 1 4】

本発明の実施の形態における第 1 1 の配信システムの構成例を示すブロック図である。

【図 1 5】

本発明の実施の形態における第 1 2 の配信システムの構成例を示すブロック図である。

【図 1 6】

本発明の実施の形態における第 1 3 の配信システムの構成例を示すブロック図である。

【図 1 7】

本発明の実施の形態における第 1 4 の配信システムの構成例を示すブロック図である。

【図 1 8】

本発明の実施の形態の構成例として示す各配信システムに共通する運用形態を表示した図である。

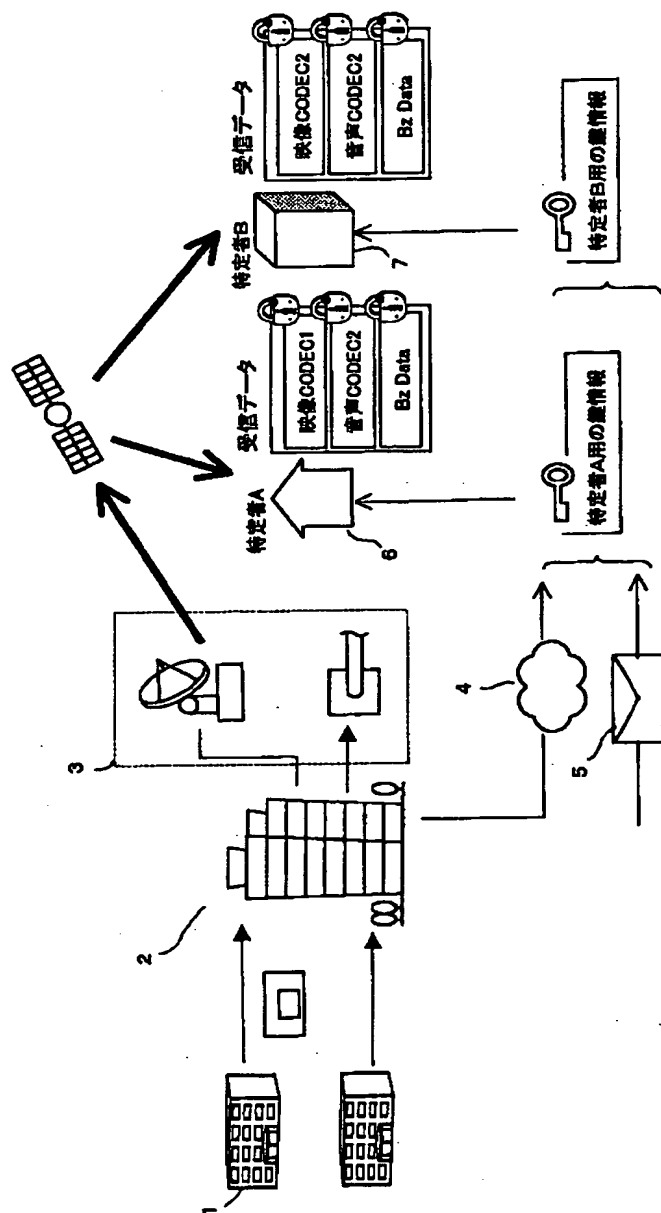
【符号の説明】

1 コンテンツサーバ、12 コンテンツ符号化部、13 暗号化部、14
送出サーバ、15 コンテンツ管理サーバ、16 鍵発生部、17 配信先管理
サーバ、18, 26 合わせ鍵生成部、19, 21, 22, 25, 27, 28,
29 書込部、20 部分鍵生成部、23 多重鍵生成部、24 鍵暗号化処理
部、31 受信サーバ、32, 38, 39, 40, 41, 42, 43 読取部、
33 復号サーバ、34 出力装置、34A デスクランブル部、35 復号機
能部、35A 復号化部、35B 鍵復元部、35C コンテンツ復号化部、3
5D スランブル部、36 スランブル制御部、37 出力ログ管理部

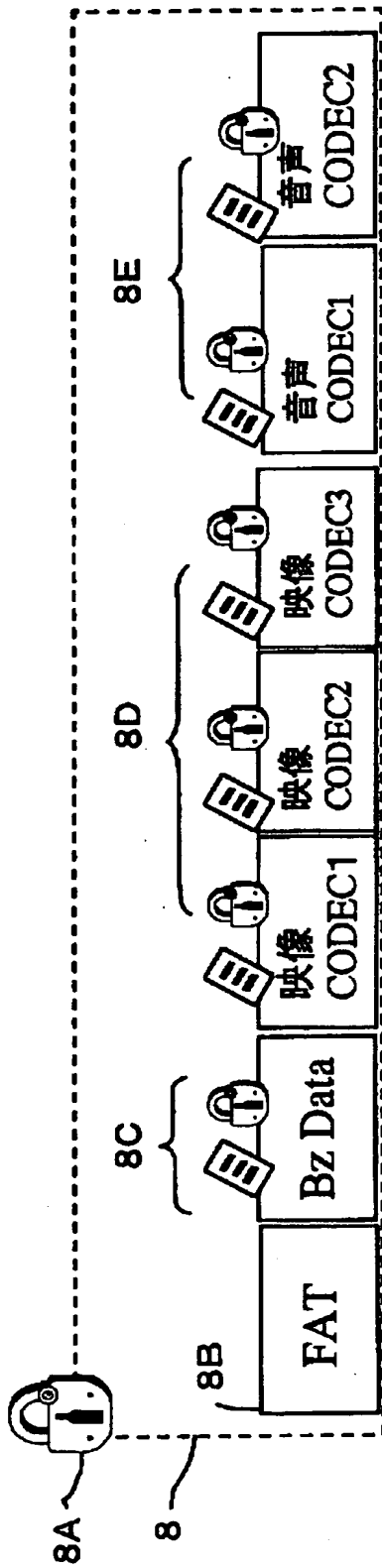
【書類名】

図面

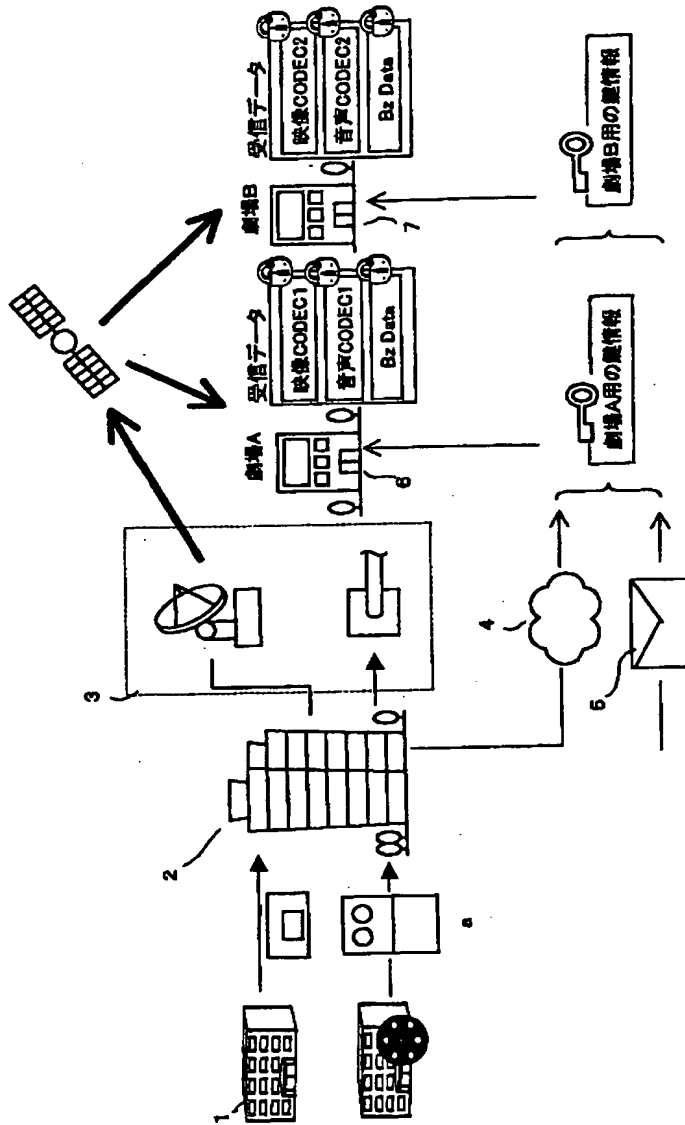
【図 1】



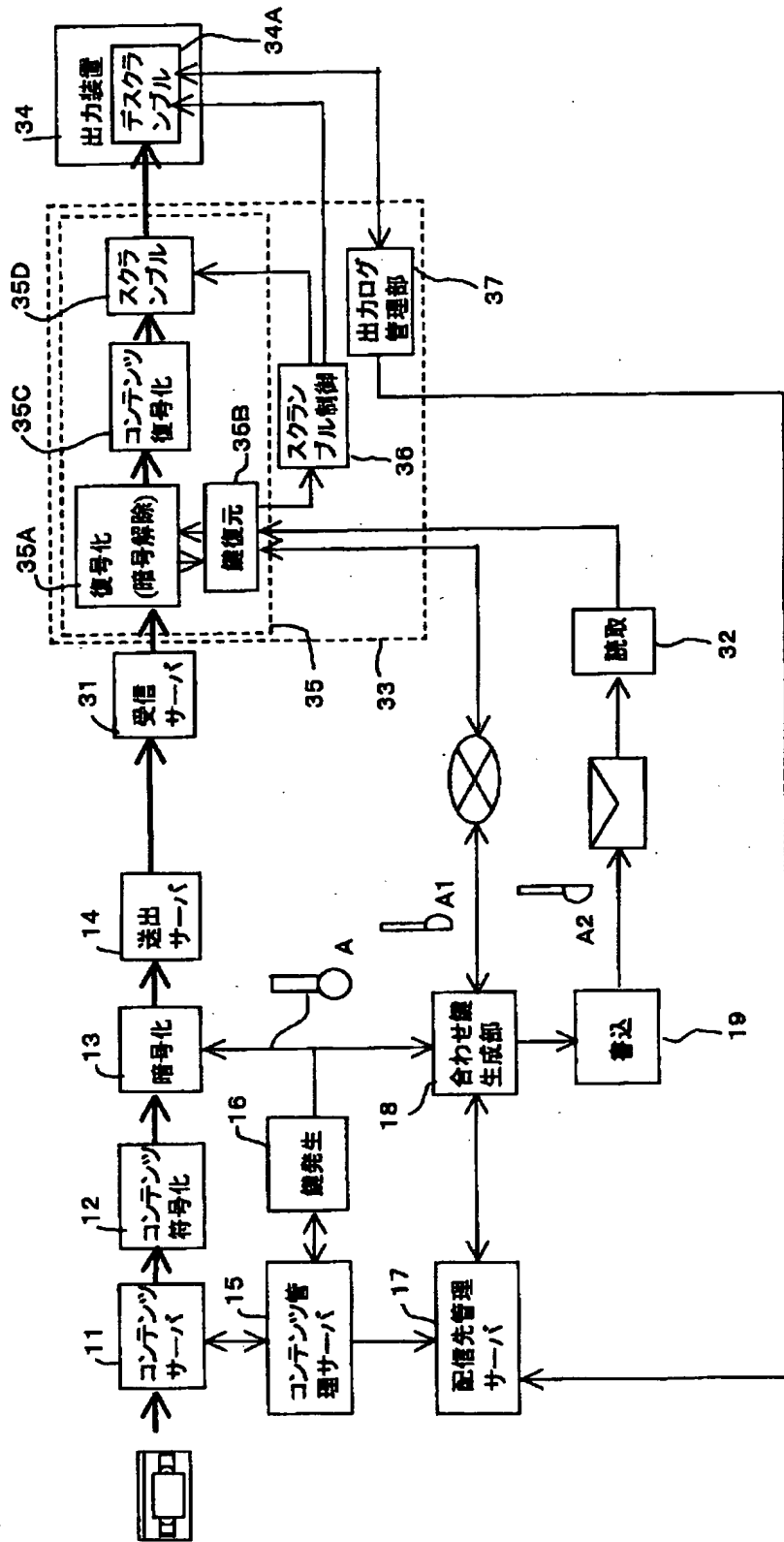
【图 2】



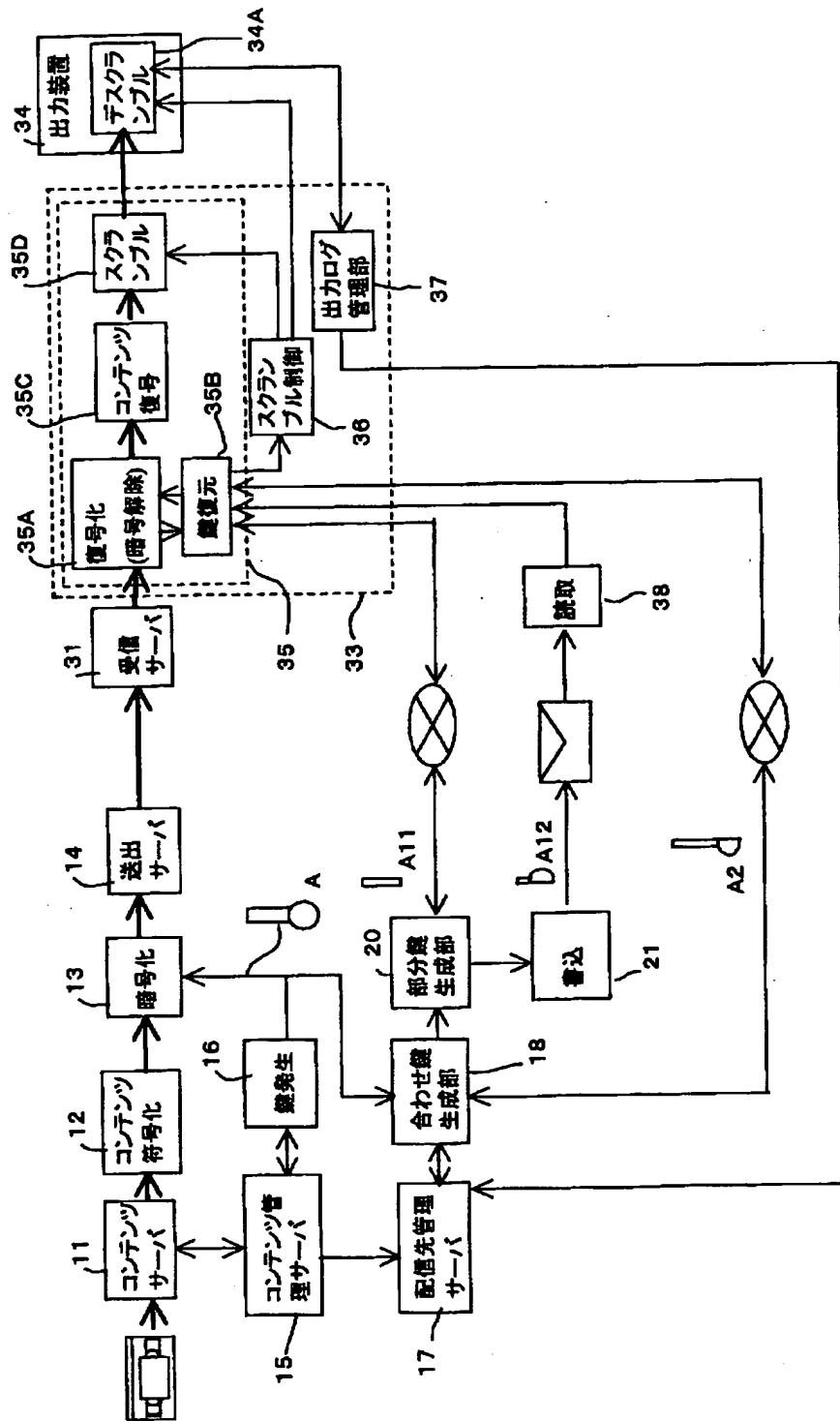
【図3】



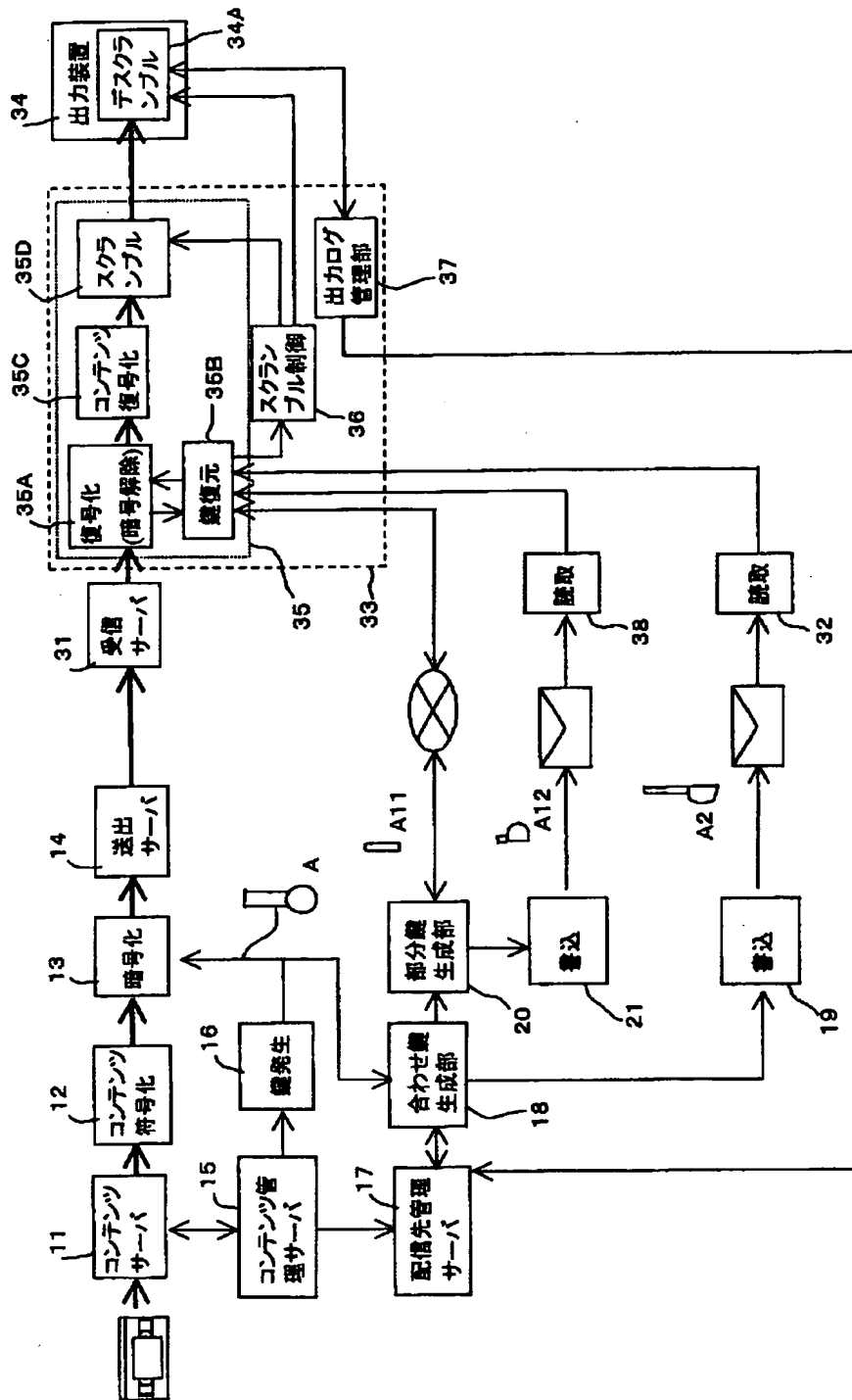
【図 4】



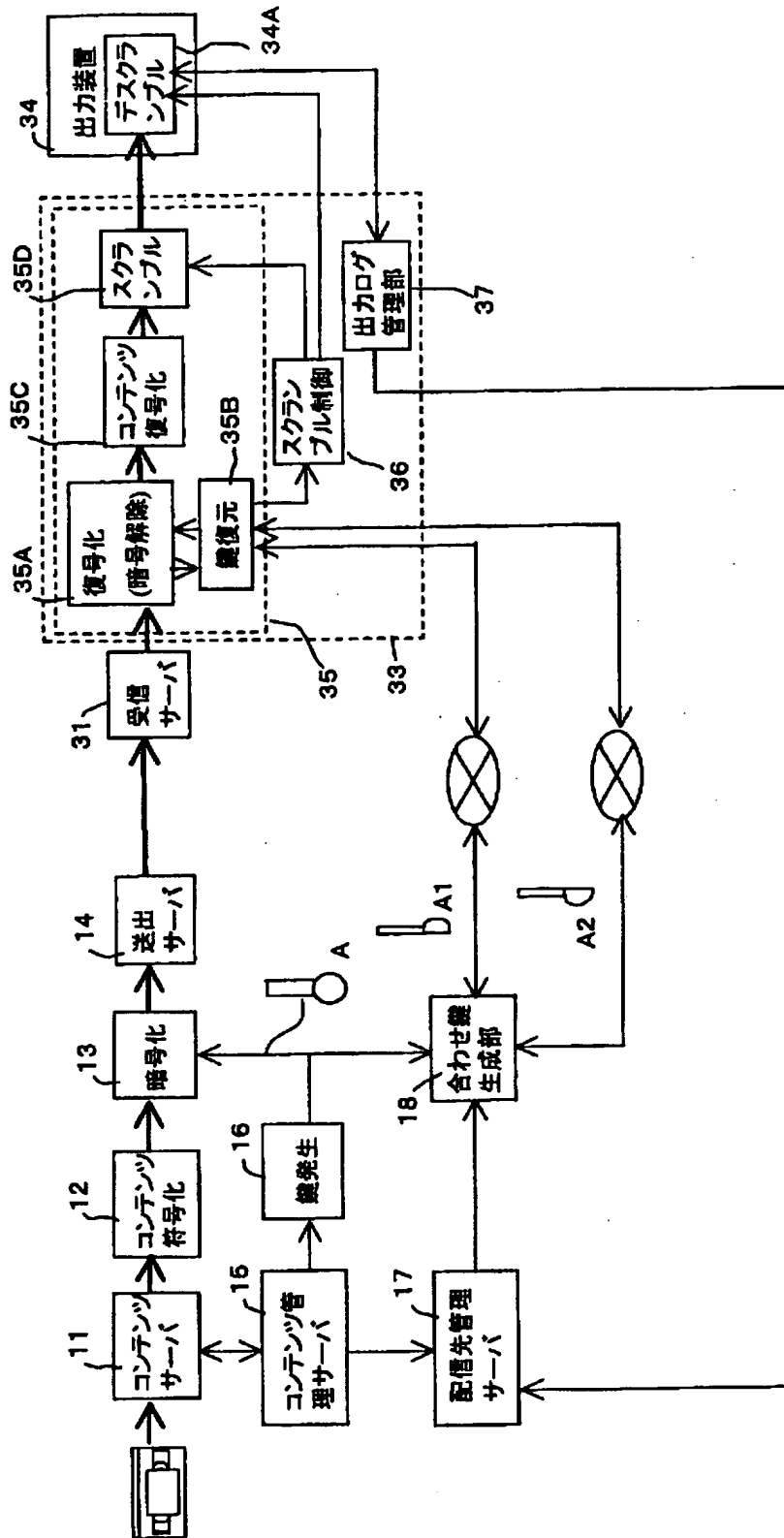
【図 5】



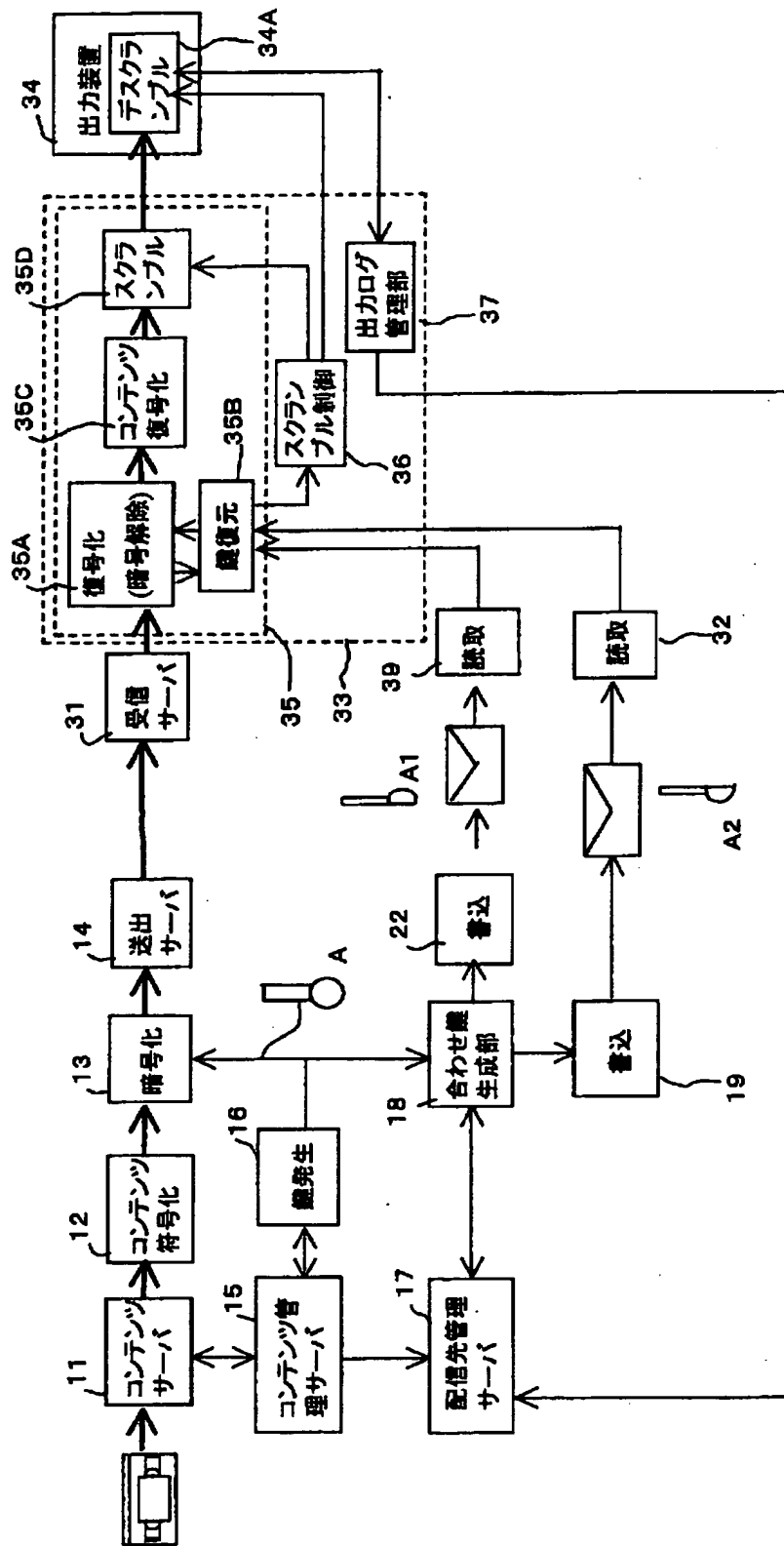
【図6】



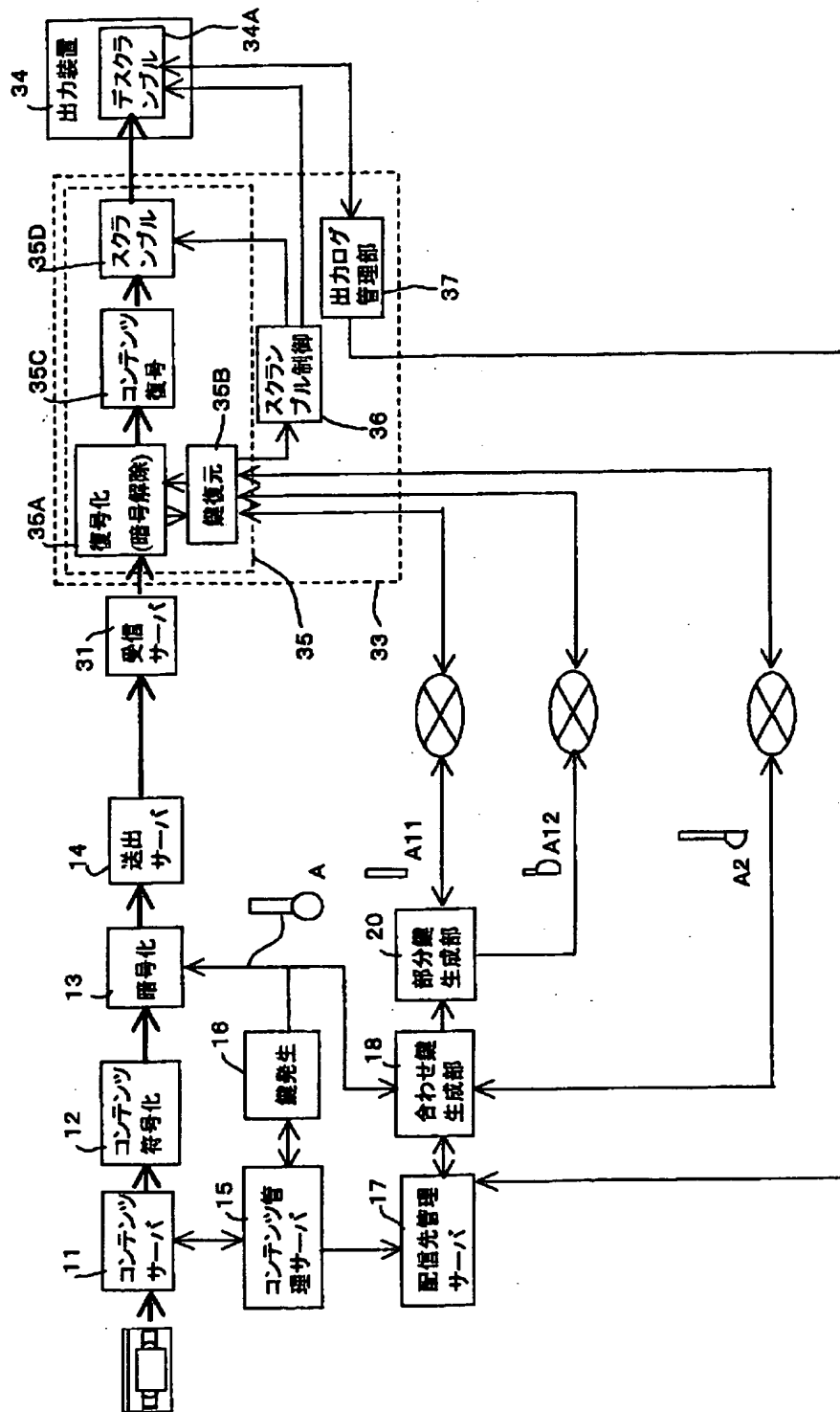
【図7】



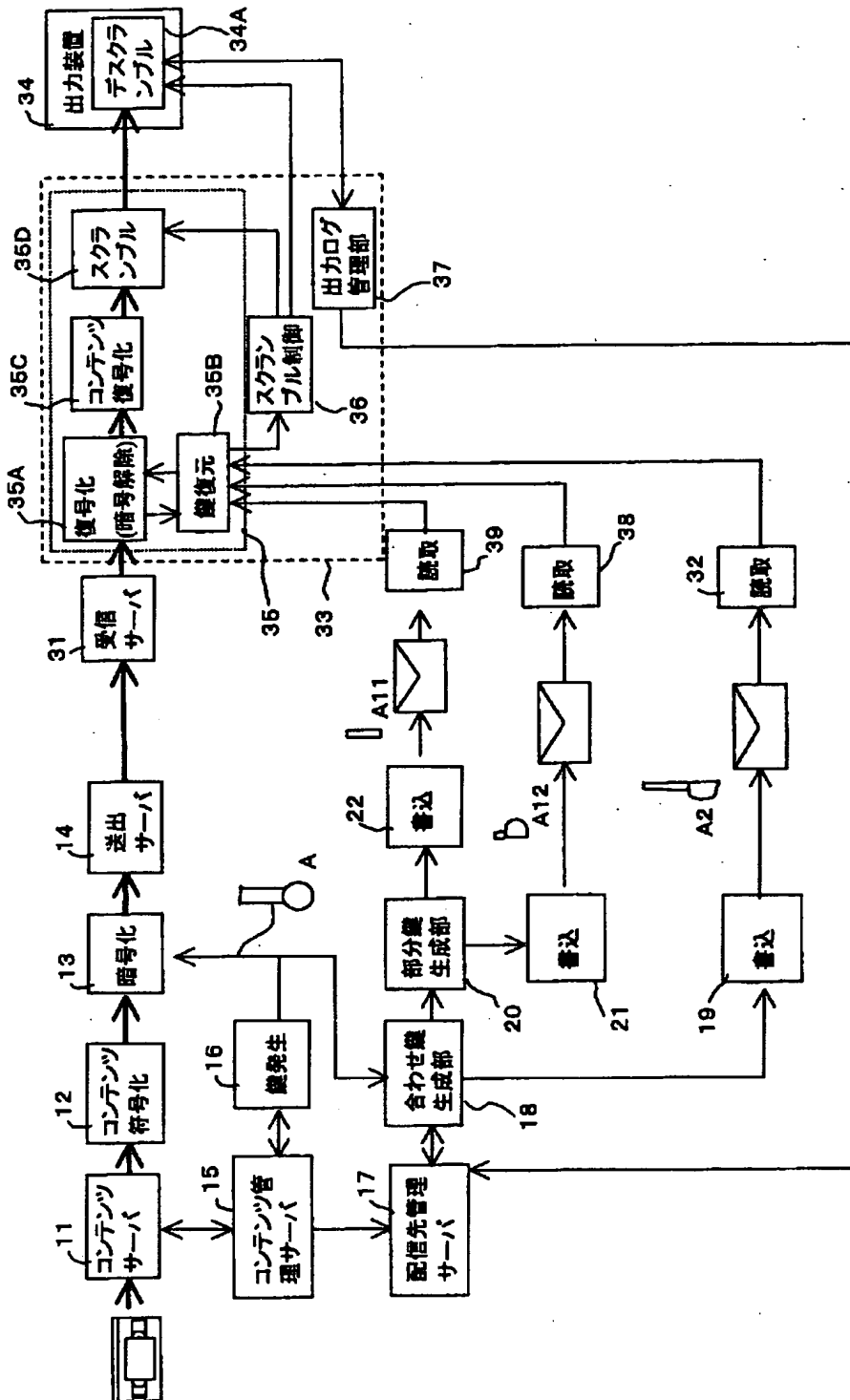
【图 8】



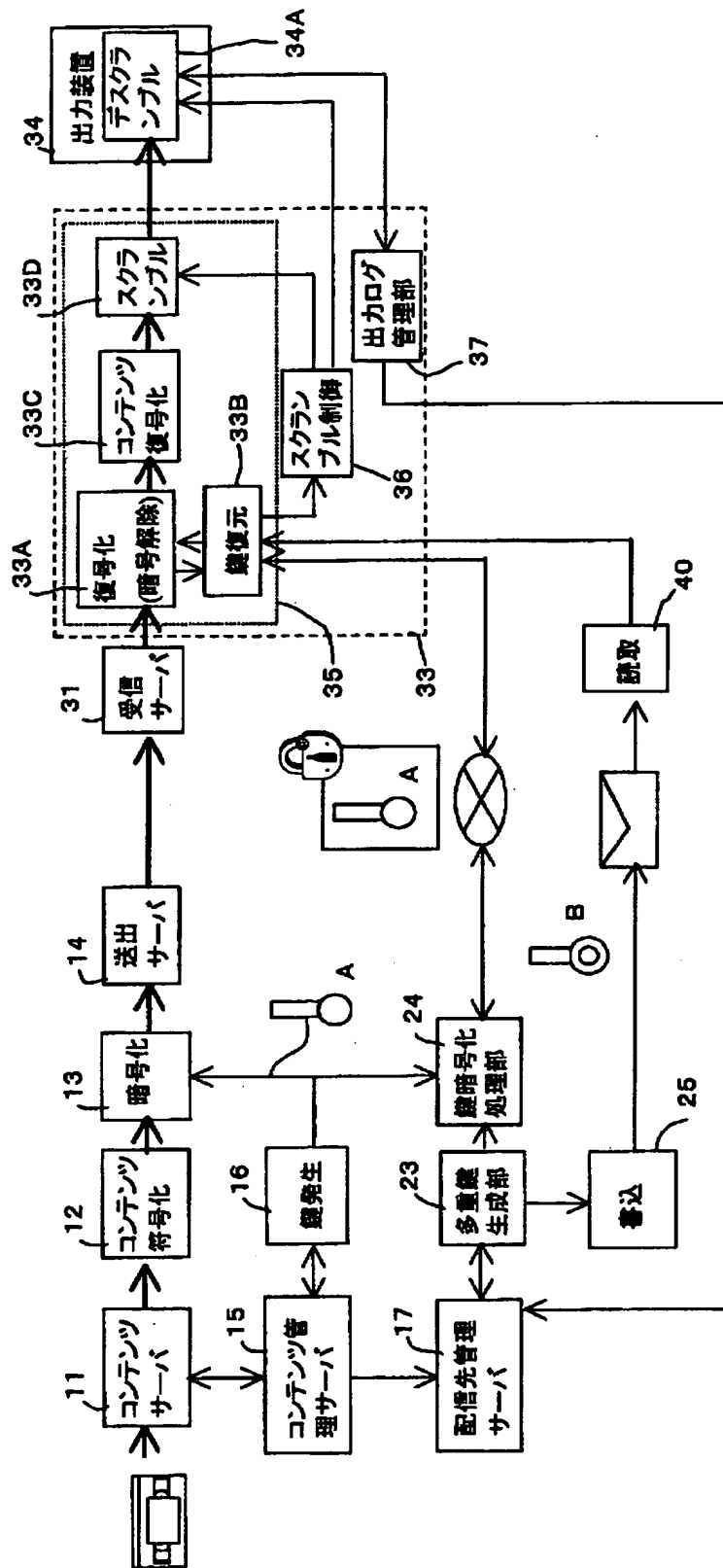
【图9】



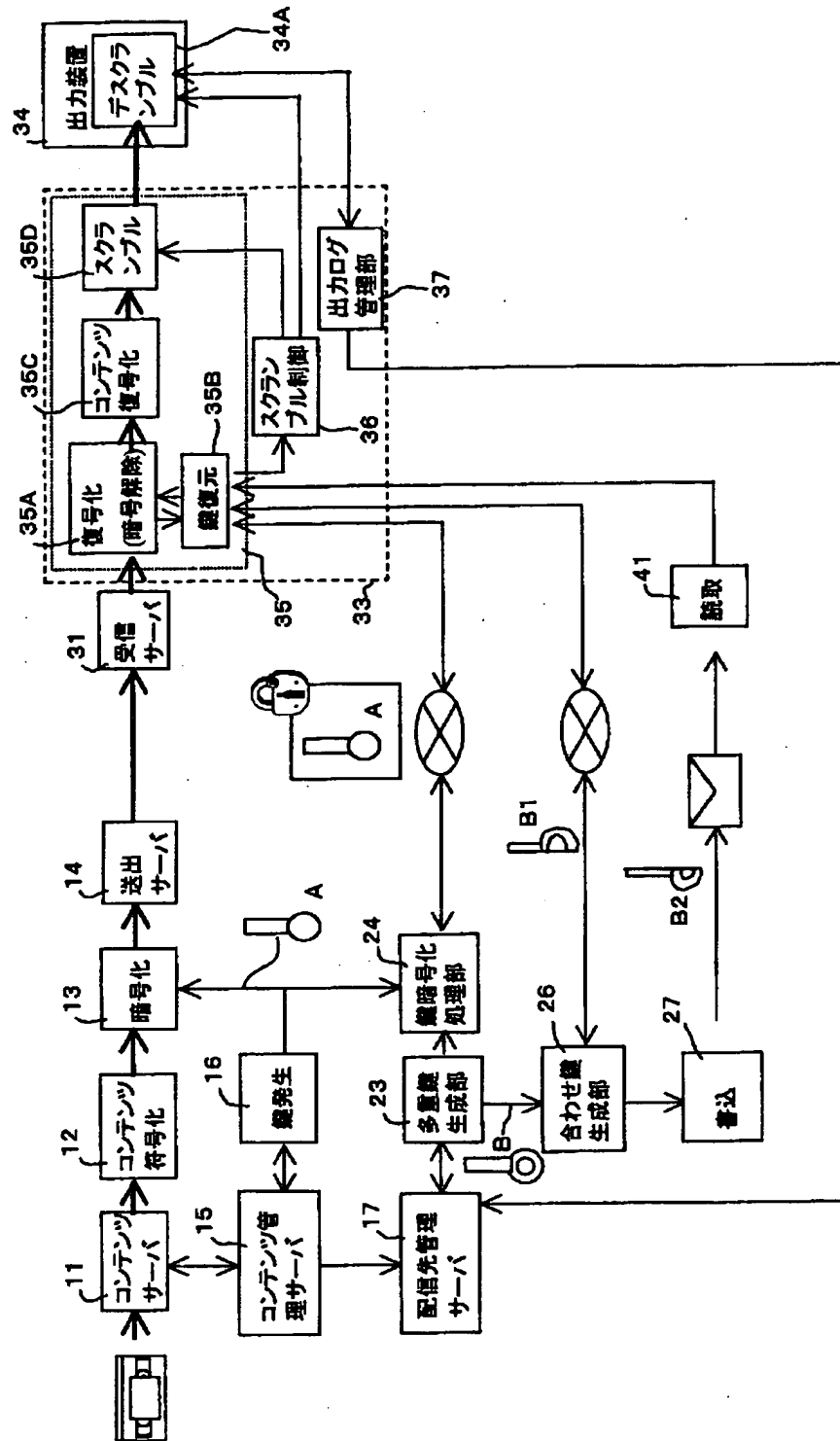
【図10】



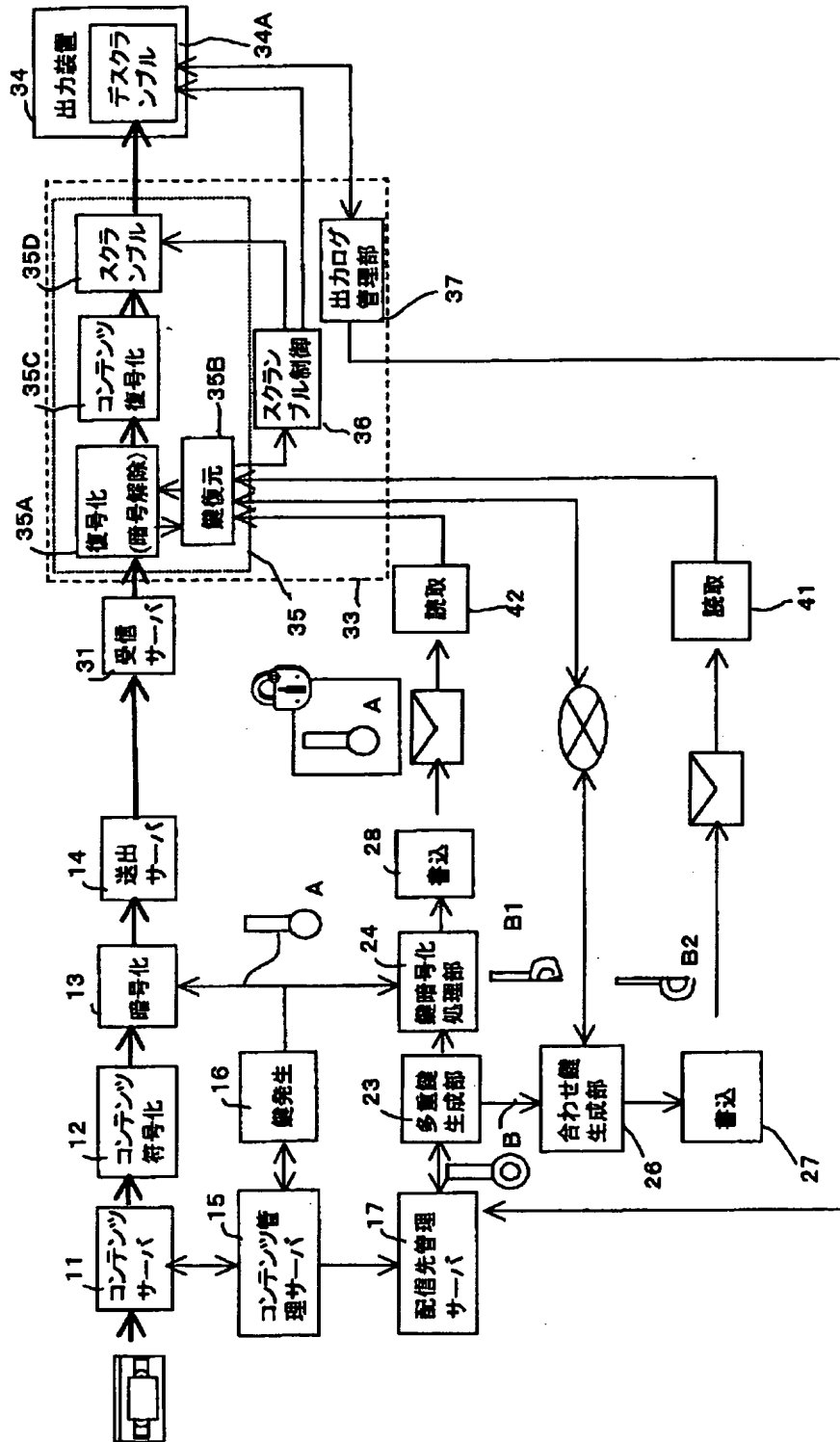
【図 1 1】



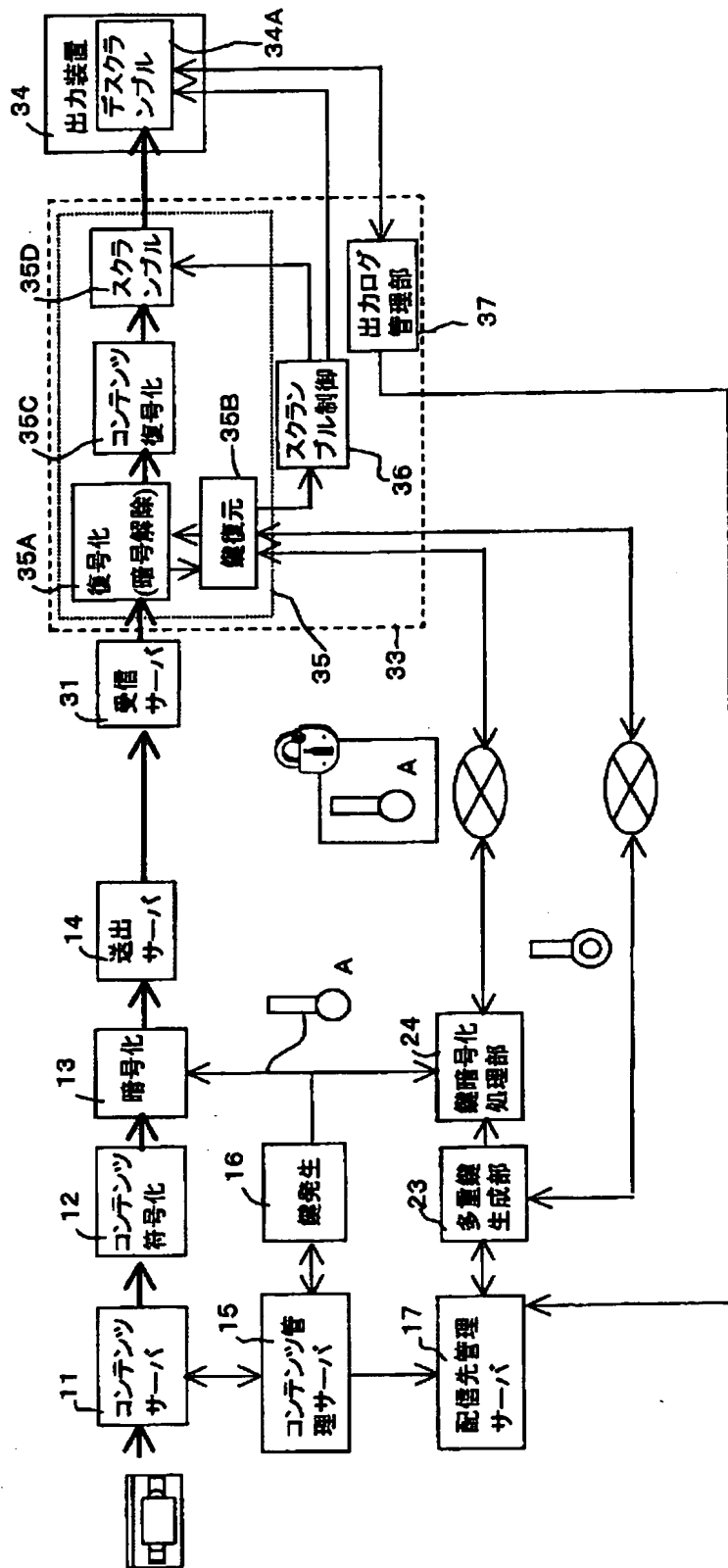
【図12】



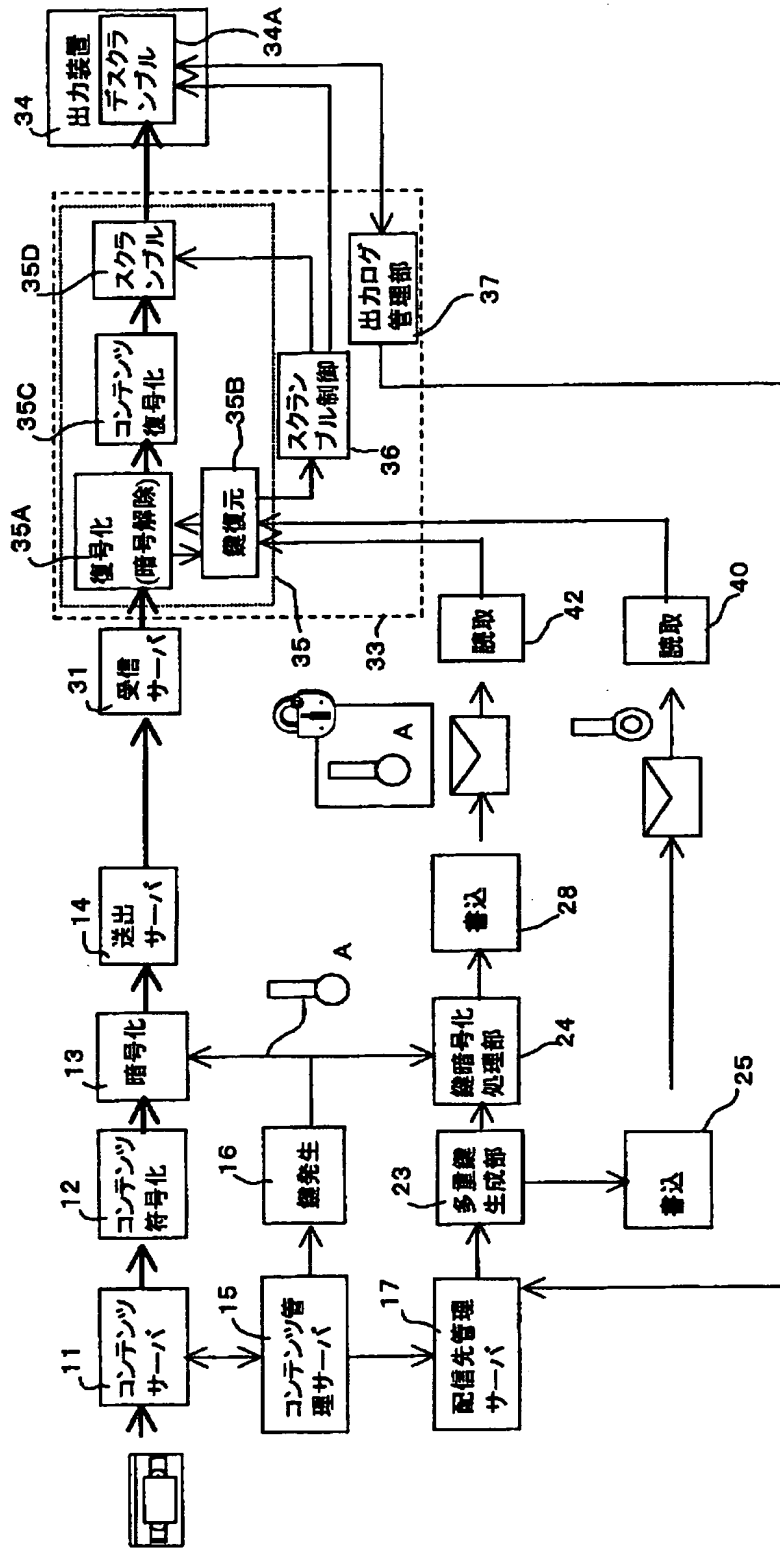
【図 13】



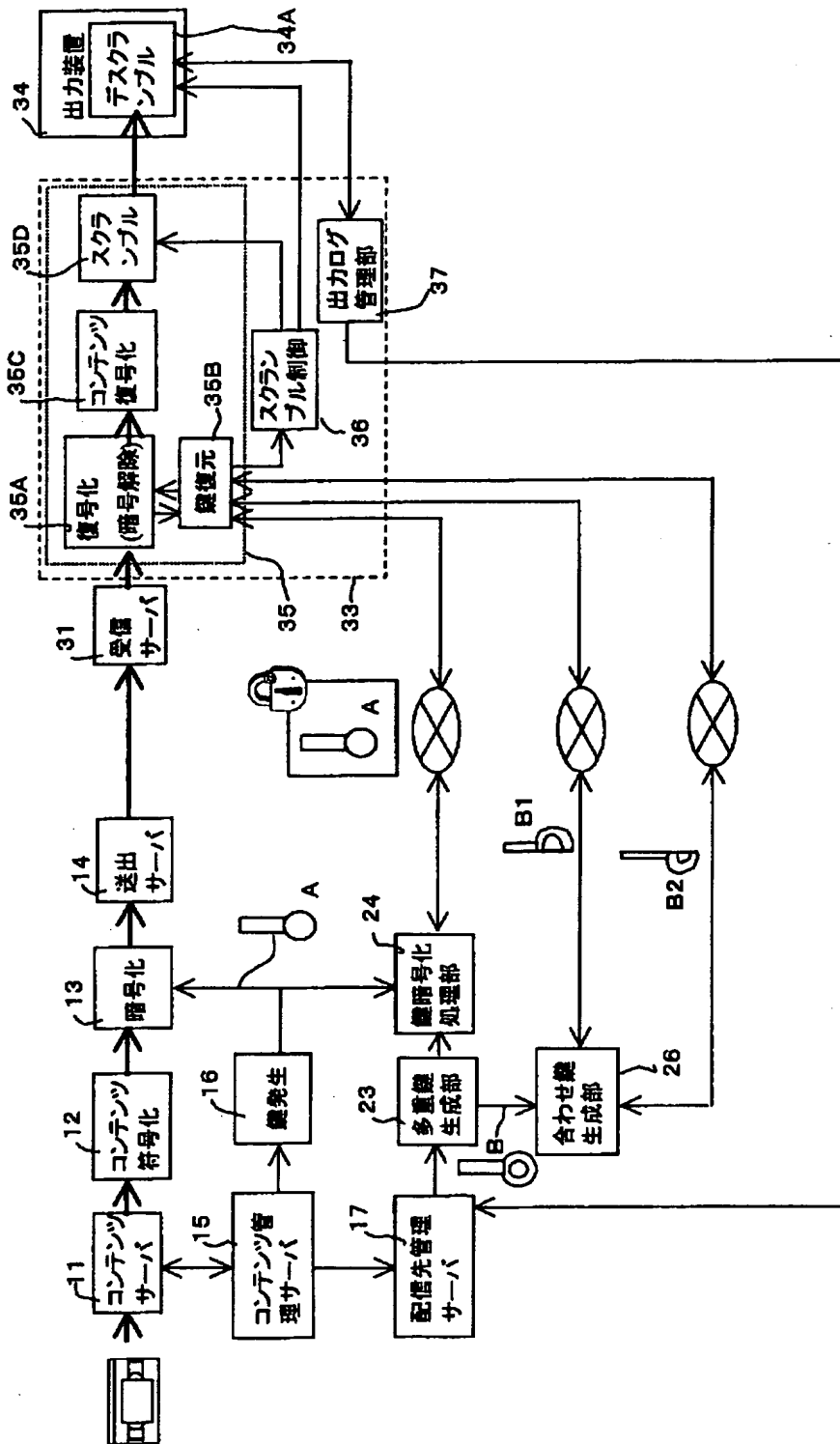
【図 14】



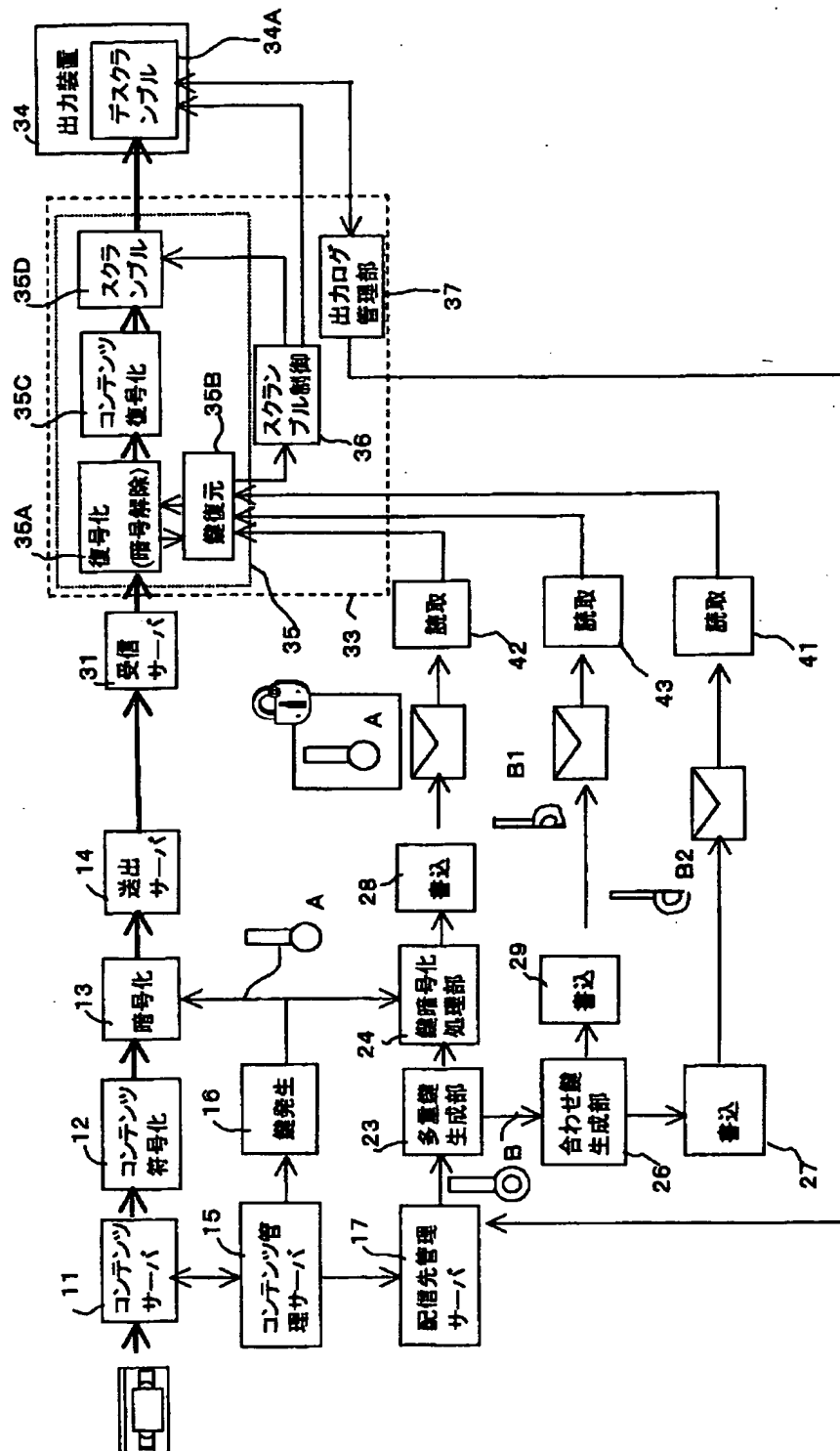
【図15】



【図16】



【図 17】



【図 18】

	暗号鍵の 発生者	符号化実 行者	暗号化実 行者	鍵情報の配信者	制作者側から 見た暗号鍵の 秘匿性	備考
1	制作者	制作者	制作者	制作者(2つ)	高	
2	同上	同上	同上	制作者(1つ)+配信者(1つ)	高	配信者が暗号化された暗号鍵を入手
3	同上	同上	同上	配信者(2つ)	中	配信者が暗号鍵を入手して鍵情報を作成
4	同上	同上	配信者	制作者(2つ)	中	暗号鍵は配信者に通知される
5	同上	同上	同上	制作者(1つ)+配信者(1つ)	中	同上
6	同上	同上	同上	配信者(2つ)	中	同上
7	同上	配信者	同上	制作者(2つ)	中	同上
8	同上	同上	同上	制作者(1つ)+配信者(1つ)	中	同上
9	同上	同上	同上	配信者(2つ)	中	同上
10	配信者	制作者	制作者	制作者(2つ)	小	制作者が暗号鍵を入手して鍵情報を作成
11	同上	同上	同上	制作者(1つ)+配信者(1つ)	小	同上
12	同上	同上	同上	配信者(2つ)	小	同上
13	同上	同上	配信者	制作者(2つ)	小	同上
14	同上	同上	同上	制作者(1つ)+配信者(1つ)	小	同上
15	同上	同上	同上	配信者(2つ)	小	同上
16	同上	配信者	同上	制作者(2つ)	小	同上
17	同上	同上	同上	制作者(1つ)+配信者(1つ)	小	同上
18	同上	同上	同上	配信者(2つ)	小	同上

【書類名】 要約書

【要約】

【課題】 不正行為の困難性とランニングコストの低減要求を両立する。

【解決手段】 復号サーバにおいて暗号処理の解除が許可されるとき、復号サーバ内で発生されたスクランブル鍵を用いて、暗号処理の解除されたデジタルコンテンツをスクランブル処理する。このようにスクランブル処理の施されたデジタルコンテンツを出力装置に与えることで、復号サーバと出力装置とを分離しても、当該伝送経路上で不正行為を行えないようにする。

【選択図】 図 4

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社